
# Espionage in the 21st century: International Legal Perspectives

**Nikolaos Zerzelidis**

Department of Balkan, Slavic and Oriental Studies and Department of International and European Studies Master's Thesis

A dissertation submitted for the MA degree in Human Rights and Migration Studies

**Supervisor: Associate Professor Nikolaos Zaikos**

## Acknowledgements

First, I would like to express my deepest appreciation to my supervisor, Associate Professor, Nikolaos Zaikos, for his precious advice and insights throughout my thesis. Without his constant inspiration, support and guidance for this challenging study, this research could not have been completed.

In addition, I would like to thank my family, namely my mom Symela, my dad Thomas, my sister Eleni and my brother Eleftherios for their constant support during my studies and my life path in general. I will be always grateful for what they sacrifice for me to develop as a person and as a professional. My love and my appreciation to them is eternal.

Furthermore, I would like to thank my friends for their support and for their insights on my research, especially my good friend and colleague Iason Chalkidis, in order to motivate me reach my limits.

Finally, I would like to express my appreciation and respect to the Secretariat of the Master's program for their constant support in administrative matters related to the students.

## Abstract

*Espionage has been a longstanding practice in statecraft, as states consider it a critical tool to safeguard their national interests. Espionage is permitted in times of war, as it constitutes a legal activity according to international humanitarian law, but in peacetime espionage is not regulated in international law. This study conducts a historical exploration of the phenomenon of espionage and aims to examine the provisions of international law on espionage and the rights of spies in IHL in order to shed light on the existing legal regime. In this attempt, it will also explore the different strands on espionage and their arguments towards the legality and illegality of espionage. Moreover, with the technological revolution and advancements in the wake of the 21st century, this research will address the new forms of espionage that have emerged, such as cyber espionage, and others that have revived, such as industrial or economic espionage, in combination with modern examples of espionage incidents, which will be also examined. This research will make an attempt to argue on the reasons that peacetime espionage has not been regulated by states. Last but not least, this area of studies is under-researched and under-developed, therefore this thesis attempts to provide insights on the international legal perspectives on espionage and expand on the current academic literature.*



**Key words:** Espionage, International Humanitarian Law, International law, legality, illegality, peacetime, wartime, cyber espionage, regulation

Contents

## Introduction

Espionage has existed as a practice and a phenomenon since ancient times. It is not easy to define the beginning of the practice of employing spies for the collection of information and intelligence, but it can be said that its roots are in the womb of human and war history. The need of humans to survive urged them to observe and study the animal kingdom and nature so as to acquire the necessary information that could be translated to a comparative advantage in the fight for food and survival. Information was critical in the process of haunting, followed by the need to learn about the organisation and the military plans of the opponent, a practise that could be accomplished with people-agents acting covertly and under despise.

Espionage has been a widespread practice in the foreign and security policy of states. Traditional espionage included the use of secret agents-spies to steal secrets of another state in a clandestine manner, which in times of war is permitted according to international humanitarian law, while in peacetime, there are no international legal provisions on the prohibition of espionage. However, espionage is clearly prohibited and criminalised in domestic criminal law. In the passage of time, the nature of espionage changed due to technological advancements, with satellites and other cyber means gaining ground as tools to conduct espionage acts remotely and even anonymously, with possibly greater damage than the traditional espionage of sending secret agents to the territory of another state at a risk of being captured. Moreover, espionage is also used to steal secrets of industrial or economic character, from either state or non-state actors and businesses in order to gain a comparative advantage to opponents, either at the state level or at the business level. Considering the fact that espionage, especially in peacetime, is a field of research that is still underdeveloped, it is assumed it would be fruitful to contribute to the existing academic debate and bibliography on such a critical field of international relations and politics that affect both state and non-state actors and their interactions.

This study will examine firstly how and why espionage was born as a necessary tool for the states to pursue foreign policy and security interests as well as its importance for the field of international relations. A historical exploration of espionage activities will be conducted from ancient times such as ancient Egypt, ancient Greece, China, the Renaissance period, the Medieval Italy, Napoleon times, both world Wars as well as the Cold war period until today. After providing some examples of espionage activities throughout history, this work will delve into the importance of espionage in the fields of international relations and strategy. Afterwards, it will explore and analyse the legal framework that exists today regarding the regulation of the status of spies and espionage activities, particularly the Lieber Code (1863), the Declaration of Brussels (1874), the Hague Regulations (1899/1907), the Geneva Conventions (1949) with the Additional Protocol (1977) as well as the Vienna Convention on Diplomatic Relations (1961). All the aforementioned legal texts, except the Vienna Convention on Diplomatic Relations, regulate espionage during wartime. However, in peacetime, as Demarest (1996) claims, international law is "*virtually unstated*" and international obligations to respect the sovereignty of a state, refraining from the threat of use or use of force against the

territorial integrity or political independence of any state according to the Article 2 paragraph 4 of the UN Charter have been challenged throughout history (p. 321).

Considering the lack of regulations on peacetime espionage, this study will explore and assess the different views and arguments that exist on the legality of espionage, particularly that is either legal or illegal and neither legal nor illegal (Radsan, 2007). After examining the different strands on the legality of peacetime espionage with examples and cases, the study will continue looking into the current forms of espionage, such as industrial, economic and cyber, presenting the challenges that these new forms have brought to international politics due to the technological advancements as well as their complexity and relationship with international law provisions. Examples of cases will be mentioned in order to be aware of some practises that are followed within these forms of espionage. Moreover, recent examples of the 21st century will be provided and examine the way states have reacted in espionage events. At this point, an analysis on the possible regulation of espionage in international law will be provided, considering the developments on espionage in the 21st century and the way ahead.

Considering the analysis that will be done in the historical and legal dimensions of espionage as well as examining the arguments on the legality of the practise, its current forms and examples of contemporary espionage acts, the study will extract some conclusions on the legality of espionage and its possible regulation from international law in the years ahead.

## Methodology

Espionage is a widespread practice in international politics as states tend to use it as a tool to protect their national interests and acquire comparative advantages in the international arena. It needs to be clarified that espionage constitutes a segment of the larger intelligence cycle and provides critical actionable information, necessary to enhance both strategic and operational decision-making of policymakers, possibly in all aspects of a state's policies. Sir Alexander Cadogan, permanent secretary at the British Foreign Office between 1938-1945, claimed that intelligence is the missing dimension of international affairs (Andrew & Dilks, 1984). Due to the increasing importance of espionage and the diversification of its nature with the development of technology, this study aims to explore the international legal perspectives of espionage in the 21st century following a qualitative analysis, examining sources of international law, including international humanitarian law (or law of armed conflict) that include provisions on espionage. The goal is to examine the position of international law when it comes to espionage and the rights of spies, which is permitted under international humanitarian law, as it is considered as a lawful conduct and a 'ruse of war', which will be thoroughly analysed in the next chapters. However, in peacetime, it is debatable if espionage is permitted or prohibited, with different strands of thought arguing about its legality or illegality for centuries.

Different disciplines have approached the issue of espionage and have provided different definitions and different perspectives on it. Therefore, this study will follow an interdisciplinary approach, with the analysis focusing on both legal texts and sources of

international law and arguments from academia, military strategists and government officials on espionage, as it is necessary for such a topic considering its complexity and the paradoxes around it. Moreover, despite the existence of bibliography around the issue of espionage in times of war, in peacetime, espionage is under-researched and underdeveloped according to the author. Despite the works of distinguished commentators from different disciplines on the issue of espionage in peacetime, which will follow, it is argued that one of the limitations of this proposed research on espionage is that there is scarce academic literature on the subject. Therefore, this thesis attempts to expand on the current literature, as well as further the academic debate on the challenging issue of espionage and the rights of spies both in times of war and peace.

## Historical exploration of espionage

Espionage is considered as the second oldest profession in human history. The earliest reference to espionage has been found in an eighteenth-century B.C. clay tablet discovered by a team of archaeologists in Syria, which records the complaint of a ruler of a city to one of his counterparts that despite the payment of the ransom, his spies were not released (Vasileiadis, 2018, p. 7). Other references related to the use of spies date back to ancient Egypt. Hieroglyphics and papyri have revealed that the pharaohs made extensive use of secret and covert agents to determine which of their subjects were not loyal to them, as well as which other tribes outside their realm were weak enough to subjugate (Vasileadis, 2018; Lerner & Lerner, 2004, p. 416). Moreover, the Egyptian spies were the first that made use of poisons using toxins derived from snake venom or plant extracts (Lerner & Lerner, 2004, p. 416). The Bible, particularly in Numbers 13:17-20, also refers to the case that before Moses planned the invasion of Canaan, he sent twelve spies in order to determine if the country was fertile or barren, if it was rich and also if the cities were walled or unfortified (King James Bible, 1769/2008).

In ancient Greece, the first recorded use of spies derives from the period during the Trojan War from both the Greek and the Trojan side (Crowdy, 2007). Both sides sent spies in order to collect intelligence regarding the intentions of the enemy, but the Trojan agent named Dolon was caught by them, who was interrogated by the Greeks and like other spies in the passage of time, he was assassinated (Vasileiadis, p, 9). During the city-states period, espionage was considered as a political and military tool, with rulers appreciating the use of agents to gather critical intelligence from rival city-states (Vasileiadis, p. 10). In ancient Greece, there was a complex and efficient system of communication between cities in the context of the art of information gathering. Postmen were chosen to relay messages, but important information was also transferred and transmitted through a system of upgraded outposts or towers, in which a form of optical telegraphy was used in order to chain the received information to their final destination (Lerner & Lerner, 2004, p. 416).

Another remarkable case of espionage from the era of ancient Greece is the case of a traitor-spy, named Ephialtes, who presented himself to Xerxes and for a high financial reward, revealed a narrow passage to the Persians, leading them from there and helping them to beat

the Spartans in the battle of Thermopylae in 480 B.C. (Vasileiadis, 2018, p. 10; Crowdy, 2007, p. 32). Another civilisation that made an extensive use of espionage activities was the Roman Empire, in which espionage was used both internally and externally of the Empire. Espionage was used internally as a tool of internal politics on behalf of rival factions, who were in conflict for power, where externally it was used for the subjugation of their neighbours and rivals (Vasileiadis, 2018, p. 10; Crowdy, 2007). It is worth mentioning that in Rome the creation of the first secret police in history (frumentarii) and the first counter-espionage service (agentes in rebus) is recorded (Vasileiadis, 2018, p. 12-13).

Espionage was not used for intelligence gathering only from the 'West', but also from civilisations outside the European continent. In ancient India, there is a reference to espionage in Vedas as a privilege for Brahmin priests (Vasileiadis, 2018, p. 16). In China, Sun Tzu in his famous work entitled 'The Art of War', he made clear his preference to the use of people in order to obtain information about the enemy situation (Vasileiadis, 2018, p. 16). He attached enormous importance to espionage, as it can be concluded from the fact that he devotes one chapter of his work to the role of spies not only for the success, but also for the danger deriving from the enemy's spies in the context of war. It is also remarkable that Genghis Khan, the Mongol Emperor, highly appreciated the role of spies in obtaining information during a war (Vasileiadis, 2018, p. 18).

Later on, in the Renaissance period, the secret services of the kingdom of England, were highly known, especially during the reign of Elisabeth I (1558-1603) for preventing numerous coups against her. The intelligence services during her reign were known to be ruthless and the agents were not randomly chosen, but among intellectual or the scientific community such as philologists, linguists and engineers, who were responsible for processing the information and reach conclusions based on it (Lerner & Lerner, 2004, p. 418; Vasileiadis, 2018, p. 20). The mastermind behind the success of the Elizabethan intelligence services was its Head, Sir Francis Walsingham, who was the sole receiver of information coming from his spies and was keeping a record of information that could be useful in the process of decision-making in the foreign policy field (Crowdy, 2007, p. 88; Vasileiadis, 2018, p. 20-21; Lubin, 2016, p. 25).

The use of spies was widely used as well during the reign of Frederick the Great of the militaristic kingdom of Prussia, who was also called as the 'Father of Espionage' (Vasileiadis, 2018, p. 21). From this historical exploration, Napoleon the Great could not be excluded, who created a massive intelligence network, which was successful both in the support of his campaigns abroad and in the extermination of the enemy's spies (Vasileiadis, 2018, p. 21).

The two World Wars are the ones with the greatest influence on the development of espionage activities both for the modus operandi and inventiveness of their methods (Vasileiadis, 2018, p. 21-30). Germany, since the first World War, had created a resilient network of secret agents, stationed in France under false identity (Vasileiadis, 2018, p. 21). During the second World War, the German secret services flourished, with the German Abwehr spreading throughout Europe, without being able to compete with the methodical and resourceful British and Soviet secret services and determine the course of war in favor of Germany (Vasileiadis, 2018, p. 22). Moreover, it has to be noted that the failure of the Germans in the field of intelligence services

can be attached to the nature of the ethnonationalist regime, particularly to the fact that Hitler used to undermine any kind of intelligence that did not confirm his beliefs (Vasileiadis, 2018, p. 23). Hitler never recognised the significance of collecting intelligence as a tool of policy making. Taking the failure of the German secret services during the second World War as an example, Hastings (2016) has claimed that democracies are able to handle critical information better than dictatorships, because they realise the importance of objective evaluation of proof and information as a tool during war (p. 482).

After the second World War, secret services experienced an unprecedented development. During the Cold War (1947-1991), the world experienced the competition between two superpowers: the US and the Soviet Union. The Central Intelligence Agency (CIA) was created in the US in the context of the US containment policy towards the spread of the influence of the Soviet Union around the world (Vasileiadis, 2018, p. 35). The main rival of the CIA was the Soviet KGB, which at that time was the biggest intelligence agency and the competition between these two intelligence services marked the whole period of the Cold War, known as the "*golden age of espionage*" (Vasileiadis, 2018, p. 37).

Taking the previously mentioned into consideration, it can be said that espionage has been always existent in the evolution of human and war history, playing either a less significant or a critical role in the outcome of a campaign or a war. It has been a predominant feature in the field of foreign policy of states to understand an opponent better and obtain clandestinely essential information to win a battle or suprise an enemy. Espionage still constitutes a tolerated practice in international politics, therefore it is paramount to examine its role in international relations and strategy in the passage of time.

## Espionage in International Relations and Strategy

After an exploration of espionage activities throughout world history, it is also remarkable to do an exploration of references to espionage made by great figures in the fields of international relations and strategy. They may differ in their approach to espionage, but consensus can be observed regarding the importance of intelligence in the process of safeguarding national interests.

Starting from the famous Indian priest named Kautilya, in his work called 'Arthashastra', he emphasizes intrigue, intelligence gathering and espionage. He places special emphasis on the intrigue in the process of affiliation with principal officials of the rival states. Deception, surprise and intelligence gathering in the context of espionage activities play a prominent role in the school of thought in the 'East', as they appear in the texts of Arab and Persian analysts of the past (Koliopoulos, 2008, p. 98-100).

For Sun Tzu, the famous Chinese military strategist, war is of vital significance and its understanding for international relations due to its accompanying benefits. For both Sun Tzu and Clausewitz, war is a cost-benefit relationship and should be chosen only when vital national interests are at stake (Griffith, 1971). In his work named "*Art of War*", Sun Tzu has clearly

stated: "*Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total*" (Griffith, 1971, p. 129). Sun Tzu highly embraces the importance of 'foreknowledge', the acknowledgement of information and its gathering through espionage (Griffith, 1971, p. 145). He argues that there are two sides to the management of information, namely its collection and dissemination. The collection of information is done in order to facilitate the decision making and the spread of information is conducted to mislead the adversary. Sun Tzu strongly defends the use of spies and informers in his work, and he makes a special reference to the types of secret agents. He categorised them according to their use. He refers to native agents (enemy's country people), inside agents (enemy officials), doubled agents (enemy spies you turned into your spies), expendable agents (enemy spies known to you who deliberately provide false information to the enemy) and living agents (those who bring news from the enemy camp) (Griffith, 1971, p. 145). Moreover, he informs us that covert operations are essential in a war and in this context, an army bases its every move on these operations. Of all those who make up the army, no one has such close relations with the commander as a secret agent, who should be rewarded more than the others (Griffith, 1971, p. 145).

Another important figure that explored espionage was Machiavelli, an Italian philosopher and diplomat during the Italian Renaissance. Machiavelli in his work he understands the concept of strategic deception. He identified deceit as praiseworthy and glorious in the context of management of war and appraised anyone that can overcome an enemy by guileful means as with force (Konstantopoulos, 2010a). Moreover, the Prussian general Karl von Clausewitz in his work "*On War*" refers to the 'fog of war', meaning the absence of reliable and accurate information during war, considering that information is the basis of military plans and campaigns (Koliopoulos, 2008, p. 150). He underlines the importance of proper processing and utilisation of critical information about the enemy in order not to create friction and confusion among the military hierarchy (Konstantopoulos, 2010a).

## Definitions of Intelligence, Espionage and Spy

For the purposes of clarity in this study, it is essential to dive into the analysis of the definitions of intelligence, espionage and spies. It has been already mentioned that the need for intelligence has always existed since ancient Egypt until today. Intelligence is highly important and critical for the survival of the states in the present-day anarchic and competitive international system. The fact that states consider intelligence as a key part of the decision-making process is axiomatic, through which they ascertain the intentions and abilities of their opponents in the international area.

The concept of intelligence is an abstract and vague concept with different definitions having been formulated by theorists and scientists from different fields of expertise. Regarding intelligence, the CIA stated that "*reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us, the prelude to decision and action by US policymakers*" (Central Intelligence Agency, 1999, p. 7). However, this definition stresses only the 'informational' aspects of intelligence. It is necessary to explore some past definitions given by either organisations or distinguished individuals in the field. According to the Dictionary of

United States Military Terms for Joint Usage (1960), "*intelligence is knowledge achieved by logical analysis and integration of available data concerning one or more aspects of foreign nations and areas and immediately or potentially significant to planning*." In 1958, a CIA operation officer, writing under the pen name R.A. Random, defined intelligence as "*the official, secret collection and processing of information on foreign countries to aid in formulating and implementing foreign policy, and the conduct of covert activities abroad to facilitate the implementation of foreign policy"* (Random, 1958, p. 76).

The definition coming from the the Dictionary of United States Military Terms for Joint Usage recognises intelligence as a product, while the second definition states that intelligence is also a process, but both overlook the counterintelligence factor. Counterintelligence is part of intelligence in an organic sense. A CIA counterintelligence officer pen-named Martin T. Bimfort amended Random's definition, due to the fact that it omits counterintelligence as a constituent part of intelligence. According to Bimfort, "*intelligence is the collecting and processing of that information about foreign countries and their agents which is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure*" (Random, 1958, p. 78). Although Bimfort's definition adds counterintelligence as a key part of the definition, it misses Random's claim that intelligence is a state activity that includes secrecy.

In its broad sense, intelligence is knowledge generated by identifying, obtaining, filtering, analysing, processing and disseminating accurate and relevant information, which is related to a decision-making process (Schaller, 2015, para. 1; Demarest, 1996, p. 322). Schaller distinguishes the generation of intelligence, depending on means and methods, into five main categories: imagery intelligence, signals intelligence, measurement and signature intelligence, open-source intelligence and human intelligence. In this context, espionage is only a specific method of obtaining information and within its limited meaning is human information collection or human intelligence (Schaller, 2015, para 1; Demarest, 1996, p. 323). While the operation of spies is usually understood under the heading of human intelligence, it is not excluded that spies use technical means or methods typically entailed in other separate areas of intelligence gathering (Schaller, 2015, para. 1).

Taking into consideration the previously mentioned, espionage or spying is a method of obtaining information. It is considered as an essential tool for the states to pursue foreign policy and security interests as well as maintain the status quo at the inter-state level. It has always been practised in international relations, both in times of war and peace. There have been various definitions provided on espionage by various agencies and entities and with different approaches to it. According to MI5, espionage is "*the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power*" (MI5, n.d.). The CIA has provided two definitions. The first one refers to espionage as "*the act of securing information of a military or political nature that a competing nation holds secret. It can involve the analysis of diplomatic reports, publications, statistics, and broadcasts, as well as spying, a clandestine activity carried out by an individual or individuals working under secret identity to gather classified information on behalf of another entity or nation*" (Espionage, n.d.).

It can be said that the traditional espionage aims for the collection of intelligence relevant to national security and especially with the target's state defence. According to the Cambridge Dictionary, a spy is defined as "*a person who secretly collects and reports information about the activities of another country or organization*" (Cambridge Dictionary, n.d.). The intelligence that a spy is aiming to collect are on the military formation of the target-state, the systems of administration, communications, recruitment and reserve of the armed forces, on developments in doctrine, tactics and equipment of the army, on the capabilities, methods and performance of the enemy's intelligence and counterintelligence services as well as on the names of senior officers and the positions of the military industry (Vasileiadis, 2018, p. 41). This intelligence is critical for an enemy state's interests that comes as a result of an espionage activity conducted by a spy recruited by a state. Although espionage is highly linked with states, there are non-state actors, such as multinational corporations, which are involved in espionage activities in non-international armed conflicts in order to attain their goals (Vasileiadis, 2018, p. 41). In this context, Black's Law Dictionary defines espionage as "*the practice of using spies to collect information about what another government or company is doing or plans to do*" (Garner & Black, 2009). Similarly, CIA has provided a second definition on espionage, referring to it as "*the practice of secretly gathering information about a foreign government or a competing industry, with the purpose of placing one's own government or corporation at some strategic or financial advantage*" (Espionage, n.d.). The second one attaches to espionage the parameter of a multinational corporation or company to gain a comparative advantage in a specific industry, which is a form of espionage in the passage of time, the industrial one, which will be analysed further in the next chapters.

Apart from the traditional espionage that aims to obtain intelligence that is relevant to the organisation, capabilities and function of a target state's armed forces, there are espionage activities that aim to collect intelligence on the scientific research, technological advancements and innovations as well as macroeconomic data that are either directly or indirectly linked to the national interests and defence of a target state (Vasileiadis, 2018, p. 42). Burn (1970) in his analysis mentions that collection targets include governments, organisations or individuals. Therefore, the espionage activities multinational corporations are engaging with, are economic, industrial or technological ones. Economic espionage is linked to intelligence relevant, for example, to the GDP, inflation or budget allocation in armed forces or industrial one to acquire intelligence that is attached to the technological innovations and developments that can provide a comparative advantage to the receiver of this critical information (Vasileiadis, 2018, p. 42).

Regarding the individuals that are conducting the espionage activities, the spies themselves, it is still questionable in research if the term refers exclusively to military personnel of the sending state or to include any civilian or military person acting on behalf of a state to secretly gather information from another or from its own (Vasileiadis, 2018, p. 42). There are definitions in the academic literature that refer to spies only as individuals coming from the military sector that engage in secret operations of intelligence gathering (Vrionis, 1960, p. 24-26). However, such approaches do not come along with the definition provided by the international humanitarian law, particularly the article 29 of the IV Hague Convention (1907) respecting the Laws and Customs of War on Land. This article provides the only definition that exists in the international law on spies. According to the article 29, "*a person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to*

*obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.*

*Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies. Similarly, the following are not considered spies: Soldiers and civilians, carrying out their mission openly, entrusted with the delivery of despatches intended either for their own army or for the enemy's army. To this class belong likewise persons sent in balloons for the purpose of carrying despatches and, generally, of maintaining communications between the different parts of an army or a territory*" (IV Hague Convention, 1907).

From the previous definition, it is observed that espionage and spies are challenging concepts that need to be further examined and reviewed according to international law and particularly international humanitarian law. Espionage is regulated by the international humanitarian law, which is part of the public international law, and this study will conduct a thorough exploration of the sources of international law related to espionage in times of war and the right of spies in case they are caught as well as shed light on the existing legal texts and explore the legality of espionage in peacetime.

## International humanitarian law/Law of Armed Conflict regulations on espionage

Before the analysis of the legality of espionage under the spectrum of international humanitarian law, it is essential to provide a definition to this important part of international law. International humanitarian law is defined as "*a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare. International humanitarian law is also known as the law of war or the law of armed conflict*" (The International Committee of the Red Cross's Advisory Service on IHL, 2022). IHL governs during armed conflicts. It comprises two key areas: regulation of the means and methods of warfare and protection and assistance to those affected by the hostilities (Haider, 2013). The two main sources of IHL are the Hague Convention (1907), defining restrictions on the means and methods of warfare and the four Geneva Conventions (1949), setting out the protection to certain categories of vulnerable people (Haider, 2013). These conventions will be analysed further in the next chapters. Moreover, a distinction should be made between IHL, which regulates the conduct of parties involved in an armed conflict (jus in bello) and public international law, as mentioned in the Charter of the United Nations, which regulates if a state may resort to the use of armed force against another state in a lawful context (jus ad bellum) (The International Committee of the Red Cross's Advisory Service on IHL, 2022).

Espionage has an ambiguous position within international law (Pun, 2017, p. 359). Although international law has previously addressed the issue of espionage during wartime and despite its relevant importance and wide use in the context of international affairs, espionage is not regulated during peacetime (Demarest, 1996, p. 330; Chesterman, 2006, p. 1072). At this point, it is highly necessary to conduct a historical exploration of existing sources of international law and other attempts that are relevant to the regulation of the status of espionage during wartime.

The 17th century can be considered as a starting point for the international legal history of espionage. Hugo Grotius, the distinguished Dutch philosopher and jurist, states that sending spies in war is "*beyond doubt permitted by the law of nations*", whose capture is accompanied by severe treatment (Kelsey, 1925, p. 655). Grotius mentions that if there are any nations "*who refuse to make use of the help of spies, when it is offered to them, their refusal must be attributed to their loftiness of mind and confidence in their power to act openly, not to their view of what is just or unjust*" (Kelsey, 1925, p. 655). Grotius's statement is still valid today, since the law of nations permits the sending of spies, but if caught, they are treated most severely from the target state. This apparent contradiction of allowing a state to send spies and another one to kill them, reflects the legal paradox in which spies are operating (Demarest, 1996, p. 331; Chesterman, 2006, p. 1078).

## Lieber Code, 1863

One of the first attempts on the codification of the laws of war was the "*Lieber Code*" in 1863. It all started around 1862, during the American Civil War, which had already been one of the biggest conflicts in human history. The lack of familiarity of the participants from both sides with the rules and customs of the just war led to the need to determine and clarify the rights and obligations of all levels of the hierarchy as well as civilians (Vasileiadis, 2018, p. 172). Under these circumstances, the then Federal Secretary of War, Edwin Stanton, under the decision taken from President Lincoln (1861-1865) authorized a commission under Professor Francis Lieber to compose, standardize, and enact the necessary amendments and changes in the rules of war, for the purpose of drafting the laws and customs of war (Vasileadis, 2018, p. 172; Garner, 1965, p. 5). Accordingly, President Lincoln approved the draft, which became binding on all federal military forces, as the Lieber Code on April 24, 1863, entitled "*Directions for the Use of the Commands of the Troops in Campaign of the United States, General Orders No. 100*" (Lieber Code, 1863).

The Code was considered as a huge step on the codification of the rules and customs of war and several European states drafted their own military manuals that adopted most of the directions of the Lieber Code (Garner, 1965, p. 5). However, the Lieber Code is not a document of international law (Demarest, 1996, p. 333). It is significant though due to its breakthrough as a primary text for the later Hague and Geneva agreements (Demarest, 1996, p. 333). One of its major points is that 'stratagems' (ruses of war) and the employment of means that are necessary to obtain information about the enemy, are considered lawful means of warfare, which is also reaffirmed in the 1907 Hague Regulations (Demarest, 1996, p. 333; Vasileiadis, 2018, p. 173-175). The Code in Article 16 defines personal deceit or false pretenses as the essence of espionage, underlines the serious threat that espionage poses and provides the heavy penalties allowed (Demarest, 1996, p. 333; Lieber Code, 1863). Deceit was considered especially dangerous in personal dealings and was justifying remarkable measures of deterrence (Demarest, 1996, p. 333). In this context, in article 101, it is mentioned that "*while deception in war is admitted as a just and necessary means of hostility, and is consistent with honorable warfare, the common law of war allows even capital punishment for clandestine or treacherous attempts to injure an enemy, because they are so dangerous, and it is difficult to guard against them*" (Lieber Code, 1863; Demarest, 1996, p. 333; Vasileiadis, 2018, p. 173). Deception was regarded so dangerous that allowed capital punishment.

The Lieber Code has some specific articles that refer to the terms of spy, espionage as well as to the treatment of a spy in case of arrest. Article 83 of the Lieber Code states that "*scouts, or single soldiers, if disguised in the dress of the country or in the uniform of the army hostile to their own, employed in obtaining information, if found within or lurking about the lines of the captor, are treated as spies, and suffer death*" (Lieber, 1863). As it was previously mentioned, capital punishment was the deterrent measure. Moreover, according to the article 88 of the Lieber Code, "*spy is a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy. The spy is punishable with death by hanging by the neck, whether or not he succeed in obtaining the information or in conveying it to the enemy*". In article 103, there is clear reference on the refusal of exchanging spies, where "*spies, war-traitors, and war-rebels are not exchanged according to the common law of war*" in order to exclude any possibility of transfer of critical information from the spy to his state of origin regarding the enemy's capabilities (Lieber Code, 1863). Article 104 introduces a significant parameter on the treatment of spies, mentioning that "*a successful spy or war-traitor, safely returned to his own army, and afterwards captured as an enemy, is not subject to punishment for his acts as a spy or war-traitor, but he may be held in closer custody as a person individually dangerous*" (Lieber Code, 1863).

Lieber was certainly influenced by the existing in force legislation that period of time on espionage in the US at the time of the Civil War, which stated *that "...in time of war or rebellion against the supreme authority of the United States, all persons who shall be found lurking as spies, or acting as such...shall be put to death upon conviction by a general court-martial"* (Anderson, 1990, p. 5). This legislation clearly states that the spy is entitled to trial before receiving capital punishment. At this point, it is necessary to interpret the previously mentioned Lieber Code. As it was stated before, there is a legal paradox on espionage (Chesterman, 2006). The use of spies is a legal practice on behalf of the states that use it to promote their goals in wartime, but the spy himself, in case he is arrested, risks being sentenced to the maximum penalty, having committed a crime under the domestic criminal law of the detaining state (Demarest, 1996). Taking into consideration Article 83, it should be noted that the role of disguise in the practice of espionage was contrary to the predictions of the just war and therefore punishable (Vasileiadis, 2018, p. 175). Hence, the uniformed military personnel that aims to obtain information behind or near enemy lines are not considered spies (Vasileiadis, 2018, p. 175). Without making the distinction between civilians and soldiers, as spies can be considered only persons who attempt to obtain information for the enemy in a secret manner, in disguise or under fraudulent pretenses, which are eventually killed (Vasileaidis, 2018, p. 175). To conclude with the interpretation of the aforementioned articles of Lieber Code, the content of the Article 104 constitutes a customary international law that is still in force today, referring to the 'reward' of a successful spy with amnesty for his previous espionage activities in the event of his subsequent capture, which is also reaffirmed in subsequent sources of the IHL that will be further explored in this study.

## Declaration of Brussels 1874

One of the first modern attempts for the codification of the laws of war was the Declaration of Brussels. In 1874, after the initiative of Tsar Alexander II, fifteen delegations of European states were gathered in Brussels to work out a draft declaration on the laws and customs of war, which had been initially drawn by Russia, following the principles of the Lieber Code

(Vasileiadis, 2018, p. 176). The draft was adopted with minor amendments and became known as the "*Brussels Declaration*"(Vasileiadis, 2018, p. 176). However, it was not ratified by the participating states as an internationally binding text, because there was disagreement between the states on the issue of dealing with the participation of the civilians in hostilities.

The Declaration of Brussels concerning the Laws and Customs of War includes several articles on the issues of espionage and the treatment of spies. First of all, article 14 states that "*ruses of war and the employment of measures necessary for obtaining information about the enemy and the country (excepting the provisions of Article 36) are considered permissible*", confirming the gradual establishment of the legality of deceptive means of procuring intelligence in the international law (Brussels Declaration, 1874; Vasileiadis, 2018, p, 176). Articles 19-22 refer to the identification and treatment of spies but are restricted only during wartime. These articles aimed to mainly make a distinction among active spies, soldiers and ex-spies, while providing no protection for spies that are caught on their own charges. Article 19 states that "*a person can only be considered a spy when acting clandestinely or on false pretenses he obtains or endeavours to obtain information in the districts occupied by the enemy, with the intention of communicating it to the hostile party*" (Brussels Declaration, 1874), while Article 20 states that "*a spy taken in the act shall be tried and treated according to the laws in force in the army which captures him*" (Brussels Declaration, 1874). Moreover, Article 21 mentions that "*a spy who rejoins the army to which he belongs and who is subsequently captured by the enemy is treated as a prisoner of war and incurs no responsibility for his previous acts*" (Brussels Declaration, 1874). Demarest (1996) claims that Article 21 provides a flexible act of limitations. Similarly, with the Lieber Code, it is recognised in the Brussels Declaration that if a spy returns to his own army, he is not obliged to any liability for his own acts of espionage in the case of his subsequent capture. The paradoxical character of espionage is present once again, considering that fact that the law of war preserves the deterrent nature of capital punishment, while rewards the spy in case of a successful mission (Demarest, 1996, p. 332).

The Declaration also made clear in article 22 to whom the espionage label could be attached. Particularly, "s*oldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies. Similarly, the following should not be considered spies, if they are captured by the enemy: soldiers (and also civilians, carrying out their mission openly) entrusted with the delivery of dispatches intended either for their own army or for the enemy's army. To this class belong likewise, if they are captured, persons sent in balloons for the purpose of carrying dispatches and, generally, of maintaining communications between the different parts of an army or a territory*" (Brussels Declaration, 1874). Similar provisions can be found also in the Oxford Manual produced by the Institute of International Law in 1880. Since the Brussels Conference of 1874 did not conclude with a legally binding text, the Institute of International Law established a committee in order to study the Declaration and submit an opinion on it (Hadjikostantinou, 2009, p. 2009). In the handbook, there is repetition of the principles of the protection against espionage on behalf of uniformed military personnel, who gather intelligence in enemy occupied territories (article 24), of the obligation to provide the right of a fair trial to the arrested spy before punishment (article 25) as well as of his immunity over previous acts of espionage in the case of subsequent capture (article 26) (Brussels Declaration, 1874). Moreover, in the manual and particularly in article 23, it was clarified for the first time that "*individuals captured as spies cannot demand to be treated as prisoners of war*" (Brussels

Declaration, 1874). This reference, in combination with the already existing subjection of spies to the jurisdiction of national courts of the states whose authorities arrested them, was another step towards the exclusion of the spies from the guarantees of the law of armed conflict and thus their legal embracement from the domestic law of the states.

## Hague Regulations 1899/1907

The next step in the development of the IHL, this time with the adoption of international legally binding texts was the signing of the Hague Regulations. One of the purposes of the Hague Peace Conferences of 1899 and afterwards of 1907 was the revision of the Brussels Declaration on the laws and customs of war that were drafted in 1874, but not ratified. The Conferences were successful in adopting the Fourth Convention and its attached regulations on the laws and customs of land warfare in 1907 (Vasileiadis, 2018, p. 179; Chesterman, 2006). These regulations make specific reference on espionage in the articles 24, 29, 30 and 31. Article 24 confirms legally for the first time that ruses of war (stratagems) and the employments of means that are necessary to procure intelligence about the enemy and the country are regarded as allowable (IV Hague Convention, 1907). It should be noted that the reference to the legality of ruses of war in article 14 is similar to the earlier documents, particularly article 14 of the Declaration of Brussels and article 101 of the Lieber Code, therefore the legality of the use of ruses of war and intelligence gathering missions during armed conflict in the body of the IHL had already been established as a customary international law, considering also espionage as a state practise in the passage of time. The article does not make any distinction between data collected by uniformed military personnel as opposed to those collected by agents in a "fraudulent" manner (Vasileiadis, 2018, p. 179).

In addition to the article that established the legality of intelligence gathering operations during armed conflict, the Conference took the initiative to provide a definition of spies and determine their treatment in the event of capture. In article 29 of the 1907 IV Hague Convention there are the three criteria of identifying an individual as a spy, which was previously mentioned in the chapter of definitions of espionage, intelligence and spies. Interpreting article 29, although not wearing a uniform while conducting intelligence operations, does not necessarily define an individual as a spy, but "*it places the burden of proof upon the suspect*" (Beck, 2011, p. 127). Articles 30 and 31 refer to the judicial guarantees for spies as well as the 'amnesty' they receive in the event of a successful operation. Particularly, Article 30 states that "*a spy who is caught on his own accord is not punished without a trial*" while Article 31 determines that "*a spy who rejoins the army to which he belongs and who is subsequently captured by the enemy is treated as a prisoner of war and is not liable for his previous actions*" (IV Hague Convention, 1907).

A continuity with the previous non-binding international legal texts is observed, since the Hague Regulations officially codified already existing international customary law (Vasileiadis, 2018, p. 180). Most of the articles use almost the same formulation as that followed in the Lieber Code, the Brussels Declaration and the Oxford Manual (Vasileiadis, 2018, p. 180). However, there is an exception, particularly in article 29 of the Hague Regulations. In that Article, the area of action of the spy is defined as the "*zone of operations*", a spatial limitation, which is not mentioned in Lieber Code (IV Hague Convention, 1907). Therefore, an agent after the ratification of the Hague Regulations would be guilty of espionage only if caught collecting information on or near the battlefield, whereas an agent tried under

the Lieber Code could be charged with espionage regardless of the area where his mission was conducted (Anderson, 1990, p. 14).

Regarding the Hague Regulations and the protection scheme towards war spies, they provide some minimal protection for war spies, but do not grant prisoner of war status. Article 30 states that a captured spy cannot be punished without a trial, which constitutes a minimal protection due to the fact that the Convention does not define 'trial' or other procedural requirements (Beck, 2011, p. 127). Moreover, taking into consideration article 31, Beck (2011) claims that the use of the word of 'rejoins' expresses an anachronistic view that war spies abandon their membership in their country's armed forces while committing espionage, even if they are obeying to the orders of the government's military that handles them assignments (p.127). Moreover, if a war spy is caught after his return to his military unit, the evidence of his guilt can be possibly weaker than when he is caught in the act (Beck, 2011, p. 127). The possibility to convict him even in the light of weaker evidence is high, if the subsequent trials against him are politically motivated and fueled by vengeance from the opponent's side (Beck, 2011, p. 127). The law of armed conflict provides protection to combatants based on their identity and acts at the time of their capture (Beck, 2011, p. 127). With the entry into force of the Regulations in 1910, without any reservation to articles 29 and 32, the definition of spies in times of war received general recognition in international law (Kish, 1995, p. 146).

## Geneva Conventions 1949 and Additional Protocols to the Geneva Convention 1977

After World War II and the atrocities committed against civilians and prisoners of war, many states sought to achieve further codification and development of the law of war (Beck, 2011, p. 127). Taking into consideration the preparatory work already done in 1912 by the ICRC, which was used as the basis at the Geneva Diplomatic Conference for the Protection of War victims of 1949, the participating states signed four important Conventions with the goal to protect the wounded and sick soldiers during war (first Geneva Convention), the wounded, sick and shipwrecked military personnel at sea during war (second Geneva Convention), the prisoners of war (third Geneva Convention) and civilians, including in occupied territory (fourth Geneva Convention) (Hadjikostantinou, 2009, p. 34). Moreover, in the common article three of the Conventions, certain fundamental guarantees were established for those coming under the authority of an opposing party during civil conflicts, which until then was considered a case that was under the exclusive concern of the involved states and their national law (Vasileiadis, 2018, p. 184).

Concerning espionage and spies, War World II made clear that spies were a category of 'non privileged' combatants, as they were vulnerable to execution in the event of capture, despite the provisions for their right to a fair trial under the Hague Regulations of 1907 (Vasilieadis, 2019, p. 184). However, only two provisions of the conventions refer to espionage. In Article 5 of the 1949 Fourth Geneva Convention Relative to the Protection of Civilians Persons in Time of War it is stated:

"*Where, in the territory of a Party to the conflict, the latter is satisfied that an individual protected person is definitely suspected of or engaged in activities hostile to the security of the State, such individual person shall not be entitled to claim such rights and privileges under the*

*present Convention as would, if exercised in the favour of such individual person, be prejudicial to the security of such State.*

*Where in occupied territory an individual protected person is detained as a spy or saboteur, or as a person under definite suspicion of activity hostile to the security of the Occupying Power, such person shall, in those cases where absolute military security so requires, be regarded as having forfeited rights of communication under the present Convention.*

*In each case, such persons shall nevertheless be treated with humanity, and in case of trial, shall not be deprived of the rights of fair and regular trial prescribed by the present Convention. They shall also be granted the full rights and privileges of a protected person under the present Convention at the earliest date consistent with the security of the State or Occupying Power, as the case may be"* (IV Geneva Convention relative to the Protection of Civilian Persons in Time of War, 1949).

In the attempt to interpret Article 5, it is necessary to mention that the article primarily had the goal to protect the military forces of the belligerents when acting as the occupying power as well as to protect the national security of the states during an armed conflict. Although this article foresees the curtailing of the ability of the captured spies to communicate, it states the right to humane treatment and a fair trial for persons arrested as spies or saboteurs. Another provision related to espionage is mentioned in the Article 68(2) of the Fourth Geneva Convention of 1949, which provides another protection for captured war spies. The Article 68(2) states:

"*The penal provisions promulgated by the Occupying Power in accordance with Articles 64 and 65 may impose the death penalty on a protected person only in cases where the person is guilty of espionage, of serious acts of sabotage against the military installations of the Occupying Power or of intentional offences which have caused the death of one or more persons, provided that such offences were punishable by death under the law of the occupied territory in force before the occupation began.*

*The death penalty may not be pronounced against a protected person unless the attention of the court has been particularly called to the fact that since the accused is not a national of the Occupying Power, he is not bound to it by any duty of allegiance.*

*In any case, the death penalty may not be pronounced against a protected person who was under eighteen years of age at the time of the offence*" (IV Geneva Convention relative to the Protection of Civilian Persons in Time of War, 1949).

This particular provision refers to the fact that the death penalty against spies in occupied territory should have been foreseen by the domestic legislation in force in the occupied state prior to the occupation. Moreover, regarding the death penalty, the limitations of the accused's lack of loyalty to the occupying state as well as his age must be taken into account. The imposition of the death penalty against the charge of espionage is accompanied with further judicial guarantees for the war spies, however they are limited.

After the Geneva Diplomatic Conference of 1949, a significant part of the law of armed conflict had been codified and developed under the prism of the War World II and other relevant armed

conflicts (Vasileiadis, 2018, p. 186). The four Geneva Conventions were not the final texts towards the development of the law of armed conflict. Their imperfections along with the longstanding presence of war and the emergence of new states in the global geopolitical landscape as a result of the decolonization process, led the ICRC to take some initiatives regarding the development of the IHL in order to reaffirm the laws of war established at the earlier international legal texts such as Hague Regulations and Geneva Conventions (Vasileiadis, 2018, p. 186). In 1973, the ICRC adopted a Draft Protocol on International Armed Conflict, in which the commentary to Article 40 made a striking clarification on the difference between espionage and reconnaissance (Beck, 2011, p. 128). The difference between these two actions is the clandestine nature of espionage. This distinction was codified in the unanimously adopted 1977 Geneva Additional Protocol for the Protection of Victims of International Armed Conflicts, particularly in the Article 46(2). The article 46(2) incorporates a revised regulation of wartime espionage, particularly who is considered a spy, his rights as well as his treatment and states:

"*1. Notwithstanding any other provision of the Conventions or of this Protocol, any member of the armed forces of a Party to the conflict who falls into the power of an adverse Party while engaging in espionage shall not have the right to the status of prisoner of war and may be treated as a spy.*

*2. A member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information shall not be considered as engaging in espionage if, while so acting, he is in the uniform of his armed forces.*

*3. A member of the armed forces of a Party to the conflict who is a resident of territory occupied by an adverse Party and who, on behalf of the Party on which he depends, gathers or attempts to gather information of military value within that territory shall not be considered as engaging in espionage unless he does so through an act of false pretences or deliberately in a clandestine manner. Moreover, such a resident shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured while engaging in espionage.*

*4. A member of the armed forces of a Party to the conflict who is not a resident of territory occupied by an adverse Party and who has engaged in espionage in that territory shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured before he has rejoined the armed forces to which he belongs*" (Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1977).

Taking the article 46(2) of the Additional Protocol of 1977 to the Four Geneva Conventions into consideration, it is observed that the captured war spy does not have the right to be treated as prisoner of war but will be treated as a spy. This article validates the present-day use of handling spies, which had been accepted as a customary international law even before its validation in IHL (Demarest, 1996, p. 337). Members of the armed forces that are captured while conducting a mission to gather intelligence in a clandestine manner with the aim to communicate this intelligence to the enemy cannot claim the right to prisoner of war status under the IHL, unless they have rejoined the armed forces to which they belong (Beck, 2011, p. 128; Schaller, 2015, para. 10). If they are captured before having rejoined their armed forces,

they may be treated as spies and prosecuted for their actions (Schaller, 2015, part. 10). Moreover, in cases of doubt whether a member of armed forces has engaged in espionage, that person shall be treated as a prisoner of war according to article 45(1) of the First Additional Protocol for the Protection of Victims of International Armed Conflicts until his or her status is determined by a competent tribunal (Schaller, 2015, para. 11).

Based on article 46(1) of the First Additional Protocol to the Geneva Conventions, a member of the armed forces that lost his or her right to claim prisoner of war status is still protected by the Fourth Geneva Convention (Relative to the Protection of Civilian Persons in Time of War) as well as by the provisions mentioned in Part IV, Section III of the First Additional Protocol (Schaller, 2015, para. 10). Those persons are entitled to the fundamental guarantees foreseen in the article 75 of the First Additional Protocol, but in cases of espionage, certain rights that are possibly exercised by the captured individual and which would be detrimental to the security of the detaining state, may be connected with derogation under article 5(1) of the Fourth Geneva Convention (Schaller, 2015, para.12). It has already been mentioned that a detained spy may be deprived of his right to communication, according to article 5 of the Fourth Geneva Convention. Despite all these provisions, article 5(3) of the Fourth Geneva Conventions stated that in each case, persons shall be treated with humanity and shall not be bereaved of their rights to a fair and regular trial. The specific guarantees over a fair trial are clearly stated in the article 75(4) of the First Additional Protocol.

Having examined the context of international armed conflict, it should be mentioned that apart from the right to a fair and regular trial as well as the prohibition of torture against the captured individual, there is not any other provision in IHL for the protection of the individual that is accused of espionage in the context of a non-international armed conflict. Therefore, the sentence of a person accused of espionage without a fair trial would be considered as a war crime that is committed either from the governmental forces or from the anti-governmental forces in the context of a non-international armed conflict such as a civil war or conflict.

Although spies are left vulnerable to death penalty according to the IHL, the IHL permits states at war to commit espionage. Article 24 of the Hague Regulations of 1907 recognises ruses of war (stratagems) as lawful means to obtain necessary information about the enemy (Beck, 2011, p. 128). The article does not provide any exceptions and it does not prohibit states from committing espionage in times of war. The acceptability of ruses of war (stratagems) is also reaffirmed in article 37(2) of the First Additional Protocol of 1977 to the four Geneva Conventions. In the article 37(2) it is stated: "*Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation*" (Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts, 1977). During armed conflict, spies are subject to punishment if captured and bear personal liability for their acts, without creating legal responsibility to their state of origin (Beck, 2011, p. 128; Chesterman, 2006, p. 1081). Moreover, the law of war foresees the ban of perfidy, but espionage is not qualified for this prohibition.

It is difficult to presume that espionage is not a necessity during war. American military author Colonel A.L. Wagner states that "*spies are indispensably necessary to a general; and other things being equal, that commander will be victorious who has the better servic*e" (Olson, 2006, p. 18-20). The view that espionage is a necessary tool of war is also reflected in Customary International Law (Beck, 2011, p. 128). Similarly**,** in several military manuals of different states, spying is not contrary to the law of war and does not constitute a war crime (Beck, 2011, p. 129; Kish, 1995, p. 148). However, espionage is considered a crime under the domestic law of the state in order to secure the national interests of the state and the interests of any kind of the armed forces (Beck, 2011, p. 129; Kish, 1995, p. 148).

Although espionage in war is not illegal under IHL and does not create grounds for complaint between states under international law, IHL does not offer adequate legal protection to war spies captured in the act (Beck, 2011, p. 126). It is necessary for the persons that are engaging in espionage to wear the uniform of their armed forces in order not to be considered and treated as spies. Spies in wartime, either civilians or military, caught in the act of espionage, are not entitled to the prisoner of war status, unless they are soldiers in uniform (Beck, 2011, p. 126). Unlike soldiers in uniform, the other individuals cannot claim the right to a prisoner of war status, therefore it should be clearly stated that the principle of distinction constitutes the legal foundation in order to be treated as a prisoner of war. Although espionage is clearly regulated during wartime in international law, particularly in international humanitarian law, there is less consensus as to peacetime espionage.

## Peacetime Espionage and different strands on the legality of espionage

It has already been stated that espionage has an ambiguous position within the international law (Pun, 2017, p. 359). Even though the act of wartime espionage is not illegal and there is broad consensus on the status of spies during times of war, espionage conducted during peacetime has received different treatment. Commander Roger Scott (1999) states that "*no international convention has ever addressed the legality of peacetime espionage*" (p. 218). Richard Falk (1962) stated on this matter that "*traditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture. And yet espionage has always played a prominent role in international relations*" (Radsan, 2007, p. 602). The words of Falk represent a fair assessment of the state of the existing literature on peacetime espionage, which is less developed than the literature on espionage during times of war.

The existing literature on peacetime espionage can be split into three different strands or groups according to Radsan (2007). One group claims that espionage is legal or not illegal according to international law. Another group states that espionage is illegal according to the regulations of international law. A third group claims that espionage is neither legal nor illegal in international law. Each strand and its arguments on the legality of peacetime espionage will be examined thoroughly in order to draw a clear view of the existing literature and perspectives on peacetime espionage.

## A. Espionage as a permissible or legal activity

There are various arguments in favour of this view. A common view is based on the lack of prohibition on espionage, which lies on the practicality of the practise of espionage as an essential tool of statecraft and pursuing national and foreign policy and security interests as well as national protection against any possible foreign intervention (Pun, 2017, p. 361). On the lack of impermissibility of espionage activities, some scholars believe that the absence of clear international regulation and states' intense engagement in espionage makes the practice accepted or permissible (Pun, 2017, p. 361). The supporters of the legality of espionage base their arguments on the *Lotus* principle from the 1927 *S.S Lotus Case* (France v Turkey), developed by the Permanent Court of International Justice (PCIJ) (Pun, 2017, p. 362). The PCIJ phrased the so-called Lotus principle as follows: "*International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed*" (Terry, 2015, p. 180). The PCIJ through the Lotus principle articulated a principle of international law that "*what is not prohibited is permitted in international law*" (von Bogdandy & Rau, 2006, para. 15). Based on this doctrine, Commander Michael Adams has claimed and urged the existence of a security-concerned "*jus extra bellum*", meaning "*the state's right outside of war*" (Adams, 2014, p. 406).

Moreover, considering the fact that treaties regulating peacetime espionage as unlawful have not been concluded and no customary international law prohibiting espionage exists, there is possibly a lacuna in international law and the PCIJ's jurisprudence should lead to the conclusion that espionage can be considered legal or not illegal (Terry, 2015, p. 180**).** This is a view that has been supported historically by different scholars and commentators such as Julius Stone (1962) and Sanchez (2017). Particularly, Sanchez (2017) has elaborated on that, claiming that international law was so vague that it was not possible for commentators that are against the legality of espionage to convincingly argue that espionage was unlawful. Moreover, Commander Roger Scott claims that "*espionage is not prohibited by international law as a fundamentally wrongful activity*" (1999, p. 218).

Historically, the absence of clear historical prohibition of peacetime espionage in international law in combination with espionage as a state practice has led commentators to claim that a customary norm for the permissibility of espionage has been created, as Baker (2004) claims that "*as a result of its historical acceptance, espionage's legal validity may be grounded in the recognition that 'custom' serves as an authoritative source of international law*" (p. 1091, 1094). Proponents of the legality of espionage have added that is and should be legal, considering the fact that it enhances international stability and peace and that spying provides the opportunity for states to gain precious knowledge and obtain critical information on another state's activities in order to react proactively in a possible ongoing crisis (Terry, 2015, p. 181). This had led some commentators such as Commander Scott (1999) to claim that the use of espionage is also a means of peremptory self-defence under both the U.N. Charter and customary international law (p. 223-224). This view suggests that espionage is a form of either arms control or conflict prevention (Pun, 2017, p. 363). An example to support the argument for the right of peremptory self-defence lies in the 'U-2' indicent in 1960.

In 1955, the CIA finished the development of the 'U-2' photo reconnaissance airplane, which was designed for intelligence gathering missions (Demarest, 1996, p. 340). Between 1956-1960, U-2 airplanes crossed the Soviet airspace in order to acquire critical intelligence for the US policymakers (Demarest, 1996, p. 340). In 1960, a U-2 airplane was shot down over the Soviet airspace and the captured pilot Gary Powers, who was a contract employee for the CIA, was not wearing a uniform and the U-2 lacked identification (Ziolkowski, 2013, p. 437). Moreover, despite the fact that Powers was an US agent, he was not lawfully within Soviet territory, therefore he was not entitled to any protection or immunity under international law (Wright, 1962, p. 14). Before the incident, the US repeatedly denied photo overflights and disavowed knowledge of their espionage agents (Demarest, 1996, p. 340). The US policy of denial lied on the inertia in international practice or underdevelopment of international law and the US policymakers were unsure of the knowledge that the Soviets possessed regarding the 'U-2' programme (Demarest, 1996, p. 340). Demarest (1996) adds that plausible denial was the global international attitude regarding spies and espionage (p. 340).

After the incident, the United States continued to deny the spying character of the overflight. Although such overflights were not formally an illegal practice, they would still be considered as unfriendly acts (Demarest, 1996, p. 340). When it became clear that Powers was not killed, the Soviets caught the Americans on an embarrassing lie and on an uncomfortable admission of the purpose of the flight, which was an act of espionage (Demarest, 1996, p. 340). The US Secretary of State justified this act of espionage as a measure to "*lessen and to overcome danger of surprise attack*" and to monitor military developments in the Soviet Union (Ziolkowski, 2013, p. 437; Demarest, 1996, p. 340). The intention was to shift international attention from the American act of espionage to the secrecy of the Soviet Union and its practice to employ secret agents. Therefore, they asserted through their act that the US has a duty towards the 'free world' (Ziolkowski, 2013, p. 437; Demarest, 1996, p. 340). Moreover, the 'U-2' influenced negatively the diplomatic rapprochement between the two countries, causing the failure of the Eisenhower-Khrushchev Paris Summit Conference (Demarest, 1996, p. 340).

If any state followed the line of argument that the US used to justify their act of espionage in the Soviet territory in order to "*lessen and to overcome danger of surprise attack*", any act of espionage would be justified from the spying state's motives such as the right to the anticipatory self-defense for any possible threat. However, international law permits military self-defence only in case of an armed attack or at least an immediate threat of armed attack and the danger understood by the US was derived from an interpretation of Soviet policy and intent and not from an immediate threat of attack (Wright, 1962, p. 18). Article 51 of the UN Charter is very clear in the case of an armed attack, in which it is stated that "*nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations"* (United Nations, 1945). Although there is a clear reference to the right of self-defence in case of an armed attack, the legality of acts of espionage cannot be derived from the right to self-defence or to the right of anticipatory or peremptory self-defence under the UN Charter and international law (Scott, 1999, p. 223-224). That right is debatable, considering for instance that the US invaded Iraq with manipulated and unconfirmed intelligence in the context of anticipatory self-defence because they decided not to wait for Saddam Hussein to abide by the UN resolutions regarding the destruction of weapons of mass destruction and this event heightened the debate for the right of anticipatory or peremptory self-defence (Radsan, 2007, p. 604).

Furthermore, on the self-defence argument, the distinguished professor Julius Stone on jurisprudence and international law, defends the permissibility of espionage, claiming that there is "*reciprocally tolerated espionage*" for mutual inspection and maintaining world stability (Stone, 1962, p. 31). He viewed espionage as a mutual check and balance game in a world where states possess weapons of mass destruction (Pun, 2017, p. 365). Moreover, he concluded that in absence of any collateral illegality on espionage, no prohibition on peacetime espionage exists (Stone, 1962, p. 34). Another commentator, such as Baker (2004) states that if self-defence is hypothetically an inherent right of a state, then the right to conduct acts of espionage is a corollary derivative (p. 1096). Taking all the arguments on the right to anticipatory self-defence into account, it can be concluded that the self-defence principle stated in the article 51 of the UN Charter can be apprehended with inherent ambiguity in international law. Nowadays, there is a different interpretation of the language of the article, mainly whether self-defence is an available option if and only if an armed attack takes place. Moreover, recent scholars have observed a shift towards an expansive view of the right of self-defence due to its more aggressive application in state practice (Pun, 2017, p. 365)

As already examined, there are scholars and other commentators that argue in favour of the permissibility of peacetime espionage, arguing either about its functional value in improving cooperation or as a means of peremptory self-defence under the UN Charter and international law, serving as a form of both arms control and conflict prevention. Moreover, there are scholars talking about the establishment of customary norm for the permissibility of espionage due to its historical acceptance and wide use in the passage of time, thus indirectly implying legality under international customary law. These views consider espionage as a lawful practice in times of peace. However, there are alternative methods and mechanisms that states can promote to ensure compliance with arms treaties and agreements, such as third-party monitoring. Moreover, it is overlooked that some states can possibly conduct espionage in collecting information for malicious purposes, such as extortion and coercion.

## B. Espionage as an impermissible or illegal activity

In this matter, Professor Deeks observes that the exact content of the principles of sovereignty and intervention can be obscure (Forcese, 2016, p. 73). The non-intervention principle was endorsed later by the ICJ in the *Nicaragua v. United States* case in 1986 (Forcese, 2016, p. 74). Nicaragua brought a suit against the United States, condemning the United States for illegal military and paramilitary activities against Nicaragua, assistance to the opposition side Contras through logistics, intelligence and material support in order to overthrow Nicaragua's Sandinista government according to the Nicaraguan claims (Fleck, 2007, p. 691)**.** As the International Court of Justice stated in its 1986 judgment in the Nicaragua case, "*the principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law*" (Nicaragua v. United States of America, 1986). The ICJ added on the principle that it "*forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy*" (Forcese, 2016, p. 74). In the Nicaragua case, the ICJ declared that prohibited interventions

included "*methods of coercion*" (ICJ Reports 1986, p. 108). On a similar approach, Oppenheim adds that in order to determine an intervention as unlawful "*the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention*" (Jennings & Watts, 1992, p. 432). The Court also invoked the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among states in accordance with the Charter of the United Nations (1970) of the United Nations General Assembly, which declares that "*no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife of another State"* (United Nations General Assembly, 1970).

Moreover, the non-intervention principle finds support from the language used in the *S.S. Lotus* case, which appears to support two diverse views on espionage, as it is mentioned also in this text as part of the arguments in favour of the legality of espionage. Particularly, the PCIJ stated that "*the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention*" (Pun, 2017, p. 367). However, the Lotus case demonstrates that the non-interference principle is not the only international rule linked to covert actions (Forcese, 2016, p. 75). According to Forcese (2016), the exercise of state power is known as "*enforcement jurisdiction*" and states that the prohibition of forced nonconsensual jurisdiction extraterritorially, meaning on the territory of another foreign state, is a fundamental principle of international law (p. 75). Any extraterritorial enforcement, without the consent of the host State, is totally unlawful, since it violates the principles of territorial integrity and political independence that are clearly mentioned in the Article 2 (paragraphs 1 and 4) of the UN Charter (Forcese, 2016, p. 75). Enforcement jurisdiction rules impose limitations on the powers some States may exercise against other states. On this matter, Chesterman (2006) claims that the limitations on enforcement jurisdiction extraterritorially "*would clearly cover unauthorized entry into territory; it would also cover unauthorized use of territory, such as Italian claims that CIA agents abducted an Egyptian cleric in Milan in February 2003 in order to send him to Egypt for questioning regarding alleged terrorist activities"* as well as *"the use of airspace to transfer such persons as part of a program of extraordinary renditions*" (p. 1082). The most famous example of exercise of covert extraterritorial enforcement jurisdiction, by spying, was the abduction of the Nazi war criminal Adolph Eichmann from agents of the Mossad, the Israeli secret service, in Argentina (Forcese, 2016, p. 76). On this matter, the Argentinian ambassador to the UN declared the kidnapping as an infringement of Argentina's sovereignty, urging the UN Security Council to adopt a resolution that called forced transnational abduction a "*violation of the sovereignty of a Member State*", which is "*incompatible with the Charter of the United Nations*" and may "*endanger international peace and security*" (Chesterman, 2006, p. 1082; United Nations Security Council, 1960).

Moreover, on the issue of sovereignty, the 1944 Chicago Convention on International Civil Aviation affirms the principle of state sovereignty over national airspace (Chesterman, 2006, p. 1082). Consequently, all states enjoy exclusive sovereignty over their land territory and associated airspace, which extends over the entire landmass to the limits of their territorial waters (Chicago Convention on International Civil Aviation, 1944). The Convention deals

mainly with civilian aircraft and includes a general prohibition on another state's aircraft flying over or landing of a foreign state without the target state's authorisation (Chesterman, 2006, p. 1083). Intentional violation such as trespassing by military aircraft of another state can be met with the use of force without warning, as it happened in 1960 when the Soviet Union shot down the US reconnaissance aircraft that conducted intelligence collection operations, which was mentioned earlier in this chapter (Chesterman, 2006, p. 1083).

The issue of sovereignty and foreign intelligence collection is also connected to the territorial waters of a country. The conduct of military intelligence collection by surface ships or submarines is subject to prohibition under the 1982 United Nations Convention on the Law of the Sea (Chesterman, 2006, p. 1082). This UN Convention protects innocent passage through the territorial sea of a state but excludes ships that engage in acts that aim to harm the defence or security of a coastal state such as intelligence collection acts (Chesterman, 2006, p. 1082-1083). According to Article 25(1) of the Convention "*the coastal State may take the necessary steps in its territorial sea to prevent passage which is not innocent*", implying espionage actions on behalf of the ships or submarines of the crossing state, therefore the target state can eventually proceed to the use of force to expel the attacking vessels or submarines (United Nations Convention on the Law of the Sea, 1982).

With various arguments in favour of the illegality of espionage presented, espionage or spying is considered as an unlawful interference or intervention in another state's territorial integrity. By spying, a state extends its scope of governmental espionage actions to influence another state's internal affairs, without respecting the target State's jurisdiction and thus violating a State's exclusive legal right of enforcement within its territory (Terry, 2015, p. 182). These arguments have been presented by statesmen of Brazil, the Bahamas and Indonesia after Snowden's revelations of the massive US NSA's spying programme in 2013 on the South American continent, invoking a breach of sovereignty and violation of international law through espionage (Pun, 2017, p. 367; Terry, 2015, p. 182).

As many acts of espionage or covert acts have a human rights dimension, there are international documents such as the 1966 International Covenant on Civil and Political Rights (ICCPR) or regional human rights conventions that protect individual rights, which put pressures on intelligence services to comply with international protections provided by the ICCPR such as the right to privacy, human treatment protection as well as the protection against arbitrary deprivation of life and the 1984 Convention Against Torture (CAT) (Deeks, 2016, p. 635; Fleck, 2007, p. 693). Particularly, provision 17 of the ICCPR states: "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . Everyone has the right to the protection of the law against such interference or attacks*" (Pun, 2017, p. 367). This has been cited by some states along with the European Convention on Human Rights to denounce the surveillance activities of the American NSA and the British GCHQ undertaken towards private individuals (Pun, 2017, p. 367-368; Deeks, 2016, p. 635). On this matter, former Brazilian President Dilma Rousseff identified the NSA's espionage, surveillance and tampering activities as a breach of international law and, which is "*an affront to the principles that should otherwise govern relations among countries, especially among friendly nations*" (Risen, 2013).

The accusations on the intelligence services' espionage activities were grave also because of the fact that ICCPR obliges governments to respect basic human rights provided in the

Covenant as well as take administrative, judicial and legislative measures to protect these rights and provide an effective remedy. Moreover, human rights groups claim that due to these revelations of the surveillance activities, ICCPR with its obligatory character and customary international law rules will generate sufficient pressure for government agencies to reconsider their practises, viewing these legal foundations as a way to regulate foreign intelligence collection, meaning espionage activities (Deeks, 2016, p. 636; Pun, 2017, p. 368). On this matter, a former head of GCHQ stated that "*as a result of pressure from civil rights organizations following Snowden, governments are rightly re-examining processes and legal frameworks for intelligence activity and seeking to improve oversight mechanisms*" (Omand, 2015, p. 17).

On the illegality of espionage, states have also accused each other of violating various legal treaties that regulate acts of espionage conducted by diplomats or embassies. Diplomacy and intelligence have co-existed since the medieval times, when the emergence of modern diplomacy in Renaissance Italy underlined the significance of employing agents to serve as negotiators with foreign states (Chesterman, 2006, p. 1087). Nowadays, there are two Conventions that regulate the diplomatic relations between states, namely the 1961 Vienna Convention on Diplomatic Relations and the 1963 Vienna Convention on Consular Relations (Vasileiadis, 2018). Article 41 of the Vienna Convention on Diplomatic Relations states that "*it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State. They also have a duty not to interfere in the internal affairs of that State"* (Vienna Convention on Diplomatic Relations, 1961). Since espionage is considered a crime in the domestic law of the victim states, it is observed that espionage through diplomats or embassies at a foreign state is also considered a crime. Despite the existence of various articles in VCDR that are relevant to espionage such as Article 22 that protects the premises of an embassy from acts of search or invasion or of Articles 27 and 40 that protect the communication of the mission from surveillance activities on behalf of the host state as well as of Article 31 that provides diplomatic immunity from criminal prosecution of a sending state's officials, Article 9 is very clear on providing the host state the right to issue a termination of a diplomat's residence in the host state without explanation and declaring him a 'persona non grata', thus requiring the sending state to recall the diplomat (Vienna Convention on Diplomatic Relations, 1961). Article 9 has been invoked after suspicions of espionage activities conducted by the sending state's officials in a foreign state, but rarely, due to the fact that diplomatic espionage has become a norm and has been a longstanding statecraft practice nowadays according to some commentators (Pun, 2017, p. 368).

The fact that there are no drawn lines of distinction between diplomatic espionage and simple intelligence gathering gives a diplomat the right of doubt to challenge his designation as a spy. This applies due to respect for humanitarian law, because the diplomat in question is not there against his will, neither fraudulently nor through false pretenses, which exempts him from being classified as a spy. So, states accept the irregular collection of intelligence on their territory by foreign diplomatic employees either silently or sometimes even without protest, with the characterization of them no longer as spies but as personae non gratae as mentioned before and finally expelling them because they did activities incompatible with their diplomatic status (Vasileiadis, 2018).

Taking into consideration all the previous mentioned on the illegality of espionage, the main arguments over the illegality lie in the non-interference and non-intervention principle as well

as the protection provided for the territorial integrity and sovereignty of a state by the UN Charter and other international Treaties. The arguments were supported by examples of cases that have depicted in practice such protections. Meanwhile, espionage activities should take into consideration human rights treaties that refer to individual rights such as the right to privacy, while some civil society organisations claim that there is a turning tide towards the adaptation of the methods that intelligence organisations adopt. Last but not least, diplomacy and espionage have gone hand in hand many centuries now, so there are also legal treaties that refer to the restrictions and repercussions of any espionage activities conducted by a foreign state's officials and embassy against the host state.

### C. Espionage as neither a legal nor an illegal activity

A third strand of thought on espionage states that espionage is neither legal nor illegal in international law (Radsan, 2007, p. 605). As Radsan mentions, there are two former officials of the CIA, namely Daniel Silver and Frederick Hitz, who have argued that it is oxymoronic about dealing with the legality of espionage in international law (Silver, 2005). About this oxymoron regarding the state of espionage in international law, these two individuals state that espionage is "*neither clearly condoned nor condemned under international law*" (Radsan, 2007, p. 605-606). Countries have less tolerance when espionage is conducted against them by a foreign state than when they commit it either against friends or foes (Radsan, 2007, p. 606). states tend to conduct espionage against other states merely for reasons of self-defence and for their own interests of national security character. This can be explained from the fact that there is neither a treaty nor a customary international rule that clearly and explicitly prohibits espionage, therefore it is not possible to argue that espionage is illegal (Baker, 2003, 1094; Radsan, 2007, p. 606). Baker (2003) particularly states that "*international law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation*" (p. 1091-1092). Baker points out the 'functional' approach on espionage, which contribute to the amelioration of the international cooperation in contemporary world issues such as terrorism, international trafficking, illegal migration, pollution and spread of diseases and pandemics (Radsan, 2007, p. 606). In this matter, Chesterman (2006) claims that espionage generates functional benefits for the international community, pointing out the benefits of sharing intelligence among states in order to develop new international norms, invoking the case for preemptive military action, specific financial sanctions against particular people or groups and cooperation for undertaking international criminal prosecutions (Chesterman, 2006, p. 1120-1126). However, Chesterman (2006) overlooks the fact that states will cooperate in sharing critical intelligence among them only when it serves particular national interests and these ways of interaction among states cannot conclude effectively and quickly an international consensus on the legality of espionage

## Forms of Espionage

### A. Cyber espionage

The analysis of some commentators on espionage such as of Stone (1962) and Wright (1962) occured at a time of technological revolution, through which the world witnessed the use of

sophisticated radio communication, satellite technology and the use of surveillance aircrafts, including the U-2 by the US in the Soviet airspace in 1960 as mentioned before (Pelican, 2012, p. 372). Stone argued about how technological growth affected and differentiated espionage as well as the types of information the states sought to serve their national interests (Pelican, 2012, p. 372-373). He understood that espionage would evolve in a way to lie in means such as satellite or sea-based reconnaissance, which would eradicate any argument on collateral illegality like the territorial intrusion of a foreign state (Stone, 1962, p. 34).

Stone was right in the argument that espionage would evolve due to the global technological revolution, but the argument that the technological development of espionage and its dependence on cyber means would diminish any arguments on collateral illegality such as the intrusion of the territory of a state is still under examination. Forcese (2016) claims that until recently, the territorial element and the violation of the territory was basic in covert actions, meaning that an agent of a state was either acting physically on the territory of another state or not, which was helpful to the analysis and assessment of the legality of espionage actions, (p. 77-78).

However, with the development of the internet and the creation of a global 'network of networks', the times changed and paved the way for a 'golden age' of espionage as Ziolkowski argues (2013, p. 425). To define cyber espionage is not an easy task. Various definitions have been provided for instance by corporate firms, security agencies, theorists and professors. This work addresses cyber espionage or 'cyber exploitation' as "*the use of actions and operations-perhaps over an extended period of time-to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks*" (Lin, 2010, p. 63). Considering the fact that NATO does not have a specific definition on cyber espionage, another definition is provided by ENISA, the European Union Agency for Cybersecurity. According to this Agency, cyber espionage is defined as "*the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation*" (European Union Agency for Cybersecurity, 2020). According to ENISA (2020), for instance, in 2019, many reports made clear that global organisations consider cyber espionage a significant and rapidly growing threat affecting industrial sectors, as well as infrastructures of critical and strategic importance across the world, including government ministries, railways, telecommunication providers, energy companies, hospitals and banks (p. 3). Cyber espionage is conducted for economic benefit or personal gain either by state or non-state actors, stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields, thus driving geopolitics in a dangerous path. It also mobilises actors from the economy and industry, which will be analysed later.

Cyber espionage is conducted by government actors or state-sponsored groups mainly, seeking to gain unauthorised access to systems and data so as to enhance their own country's national security interests, economic competitiveness as well as military capabilities and strength (Maras, 2016). First of all, the importance of committing cyber espionage and its relevance to national security lies in the fact that it reduces risks to intelligence services regarding the use of spies, for instance to be caught in the territory of another state or with regard to 'turned' spies and traitors (Ziolkowski, 2013, p. 425). Moreover, cyber espionage provides the opportunity for large-scale out-sourcing of information and offers new possibilities and advantages in terms of ease, speed and inexpensiveness of intelligence collection with regard

to the amount of information to be gathered (Ziolkowski, 2013, p. 425). In this context, the deterrence of cyber espionage operations has been a new priority for the national security of states. Due to the ease of cyber espionage operations, this new concept of espionage has escalated the 'threat picture', considering the effectiveness of espionage committed by cyber means (Ziolkowski, 2013, p. 447). Moreover, the target state does not have the opportunity to prosecute and imprison the 'online' spies engaged with cyber espionage against its cyber capabilities, due to the lack of physical appearance of spies in the target state's territory (Ziolkowski, 2013, p. 447).

Ziolkowski (2013) also argues that the espionage activities have acquired an economic focus from a politico-military since the end of the Cold War (p. 447). This applies not only to the Western democracies, but also to less developed countries, which invest funds to raise their cyber capabilities and resort to cyber espionage in order to steal technological knowledge and modern devices that they could not acquire otherwise, meaning indirect economic loss to the target states and intrusion of their national cyber means (Ziolkowski, 2013, p. 447). Therefore, economically motivated cyber espionage is a growing threat for all states that gains ground in the setting of new priorities in national cyber strategies, as they are vulnerable to cyber espionage due to the sophistication of IT means used and the reasons explained later such as the effectiveness, speed and ease of data collection methods mentioned before.

Considering the previously mentioned, as cyber espionage is presented as a mean to undermine the national security and stability of a target state, either directly or indirectly, it is observed that the term national interests is broader than national security, due to the fact that national interests include security, public safety, natural resources and other vital interests of economic character. Due to the growing relevance of cyber espionage activities that drove the the greater inclusion of national economic interests to the national security scheme, there is the question whether the simple act of a state using its cyber capabilities on its own territory in order to penetrate a server or in general the cyber means in the territory of a foreign xtate violates the target state's sovereignty. This question leads to the examination of whether the cyber invasion or penetration of another state's cyber means breaches international law with regard to 'use of force' against the territorial integrity or political independence of any state mentioned in the Article 2(4) of the UN Charter and to 'armed attack' pursuant to Article 51 of the UN Charter.

According to Forcese (2016) and Pun (2017), the former question was addressed partly in the 2013 Tallinn Manual on International Law Applicable to Cyber Warfare, which is an extensively cited document on cyberwarfare, as it represents the collective view of international experts gathered by the NATO Cooperative Cyber Defence Centre of Excellence. Despite its non-binding nature as an instructional manual, it constitutes the most comprehensive approach on the topic. The Tallinn Manual defines cyber espionage as "*any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating to the opposing party*" (Schmitt, 2013, p. 159). It is observed that in the Tallinn Manual, cyber espionage is mentioned in the context of armed conflicts and not in peacetime. The Manual does not make an analysis of cyber espionage in times of peace, and this is due to the argument that there is an "*absence of a direct prohibition in international law on espionage per se"* (Schmitt, p. 50). According to the Manual, "*a cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no*

*physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty*" (Schmitt, 2013, p. 16). Moreover, it argued that "*intrusion into another State's systems does not violate the non-intervention principle . . . even where such intrusion requires the breaching of protective virtual barriers"* (Schmitt, 2013, p. 44-45). It should also be noted that the Manual did not address whether remote intrusion into the territory of another state constitutes an exercise of enforcement jurisdiction.

Considering the previously mentioned, in determining the legality of intelligence gathering through cyberspace, there is still ambiguity whether or not it breaches a state's territorial sovereignty despite that there is no physical presence of another state's agents. Moreover, another legal consideration in the context of acquiring processed intelligence in cyberspace is that of privacy protection. This issue has arisen due to the revelations of major cyber espionage operations conducted either by state or non-state actors. Some remarkable examples of such operations are *GhostNet,* which is considered to have successfully infiltrated computer systems of embassies, foreign ministries and other government offices in 103 countries and mass surveillance programmes of the US, particularly the NSA, under the name "*PRISM*" and "*Boundless informant*" that included cooperation with tech giants such as Microsoft, Apple, Google, Facebook, Yahoo, YouTube, Yahoo, Skype, AOL and PalTalk (Ziolkowski, 2013, p. 426). Another case derives from the Russian-Georgian conflict in 2008, when Russian hackers engaged in "*information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks*" (Hollis, 2011). Moreover, the case of the alleged Russian cyber attack in the US elections of 2016 should be mentioned, where Russia interfered particularly in the campaign of the Democratic Party's candidate Hilary Clinton, sending 'spearfishing emails' to spread propaganda and hacking the voters' data in state websites (Lipton, Singer et al, 2016).

This issue of privacy protection arises not because it might prohibit the acquisition of processed information in cyberspace, but rather it might introduce limitations or even thwart it if it is determined as illegal. This debate also includes whether Article 17 of the International Covenant on Civil and Political Rights (ICCPR) could be applied to citizens outside the territorial jurisdiction of the acting state, but ICCPR's Article 2 provisions apply to individuals within the state's territory and subject to its jurisdiction. Therefore, ICCPR is not applicable to citizens of a state that are monitored by a foreign power that conducts cyber espionage against them. Considering this fact, further development of the ICCPR's international jurisdiction is needed so as to address the legality of transnational surveillance, which is unregulated by international law, except the provisions that exist regarding communications in diplomatic missions.

The issue of cyber espionage has arrived in the geopolitical arena as a new threat to the national interests and security of all states. The vulnerability of the states to address cyber attacks is an issue that is getting gradually addressed by the national cyber security strategies around the world. The states have now to address not only physical threats, but cyber threats and the victim states regularly do not know who is behind the intrusion of their national cyber means or even the intention and its potential destructive capacity. The shift of perceptions on national security due to the emergence of the cyber attacks has driven many commentators to argue for or against the determination of cyber attacks as a breach of international law due to the remote intrusion of a state's territory and political sovereignty. This issue is debatable as it has been argued in an international collective attempt, that of the Tallinn Manual, which addresses the issue in the

context of an armed conflict. Due to the ease, speed and effectiveness of cyber espionage operations that have the capabilities to obtain mass amounts of data and cause great destruction at a national and international level, the legality of such operations and its effects on the international stability should be re-addressed in order to adapt to the new realities and trends that cyber attacks have created.

## B. Economic and Industrial Espionage

Trade, like war, is a field of opportunities, confrontations, risks and crises. Both states and businesses develop their competitive strategies in order to attain their goals. Their survival depends on choosing the right strategy. The structure of the system in which both states and companies operate affects both their position and strategic behaviour, therefore the analysis of the market is essential to determine the opportunities, risks, constraints and weaknesses.

Nowadays, information wars are the new reality, since information determines perceptions, opinions and power**.** Information or the lack of it, is a critical factor that determines the probability of success. According to Sun Tzu, if sufficient and reliable information is available, victory is certain (Griffith, 1971). Sun Tzu's ancient wisdom for conducting traditional battles is applicable likewise in the field of business technology and industry. Therefore, states and businesses today tend to conduct espionage in order to gain a comparative advantage in comparison with others.

Industrial, economic, corporate, or technological espionage are forms of espionage conducted for commercial purposes rather than for purely national security purposes. However, there is a definitional confusion between economic and industrial espionage, because this subject of studies is under-researched and because different academic fields such as sociology, criminology and law use a different terminology and adopt a different approach on those forms of espionage (Konstantopoulos, 2010b, p. 9). Porteous (1995), a security analyst of the Canadian Security Intelligence Service, has defined economic espionage as "*clandestine or illicit attempts by foreign interests to assist their economic interests by acquiring economic intelligence which could be used to sabotage or otherwise interfere with the economic security of another country*" (p. 297). Regarding this definition, he clarified the term 'economic intelligence' as "*policy or commercially-relevant economic information, including technological data, financial, commercial, and government information, the acquisition of which by foreign interests could, either directly or indirectly, assist the relative productivity or competitive position of the economy of the collecting organization's country*" (Porteous, 1995, p. 297).

After providing a definition of economic espionage, it is essential to clarify that industrial espionage refers to the collection and analysis of information on behalf of a company against another company, where the collection process is conducted using clandestine means (Konstantopoulos, 2010b, p. 11). This form of espionage is conducted usually by an entity of the private sector, while economic espionage is conducted by a government of a state through its secret services, either against another state or against private companies in order to provide critical information to indigenous companies and acquire a comparative advantage in the international arena (Konstantopoulos, 2010b, p. 11).

Regarding the historical background of economic espionage, its roots are dated back to ancient times, when the Children of Israel, after the order given by Moses, wandered around Sinai to "*spy out the land*" and extract conclusions over both the military and economic capabilities of the land of Canaan (Konstantopoulos, 2010b, p. 13). Another example can be invoked from ancient Greece, when in 416 B.C, the city-state of Athens sent a delegation in Eugesta in order to learn about the economic capabilities of the town in order to finance a joint military operation (Gerolymatos, 2001, p. 30). However, the delegation of the Athenians was misled by the citizens of Eugesta about the real economic capabilities of the town by falsifying their real capacities and resources. Modern examples are dated back to the period of World War II, when the US Board of Economic Warfare was tasked to study the Japanese economy and analyse the role of Japanese resources and commodities (Konstantopoulos, 2010b, p. 15). A more recent example is dated back to the end of the 1980s, when French secret services were discovered to conduct economic espionage against US Computer companies such as IBM and Texas Instrument, causing protests from the US (Ziolkowski, 2013, p. 439). Another example is the discovery of the US that Israeli officers acquired clandestinely technological information on an US airborne spy camera system, causing the denial of the Israeli side, but there was not any official statement or protest from the US (Ziolkowski, 2013, p. 439). A very recent example comes from Snowden's revelations over NSA spying on foreign companies (Pun, 2017; Terry, 2015). It should be noted that according to US CIA reports, over 90 countries have conducted economic espionage against the US companies (Ziolkowski, 2013, p. 439). This is based merely on the underestimation of the economic capabilities of other countries from the US themselves, since they have missed the fact that despite their economic and technological superiority, they are still vulnerable to other countries' espionage acts, which aim to balance this superiority in the economic field. It should be highly noted that economic espionage is also conducted among allies and not only among enemies.

Regarding industrial espionage incidents, for instance, in 1993, Opel automobile manufacturer accused Volkswagen of industrial espionage after Opel Vice President of Procurement of US operations Jose Ignacio Lopez and seven other executives moved to Volkswagen (Brown & Swoboda, 1996). Lopez was accused of unveiling trade secrets from Opel to Volkswagen and the case was finally settled in 1997, resulting in one of the biggest settlements of industrial espionage. Another example is the accusation of the former Brazilian President, Dilma Rousseff that NSA allegedly conducted industrial espionage against the biggest Brazilian oil company named Petrobras (Boadle, 2013).

The legality over industrial and economic espionage operations is doubtful and the international regulations on property rights protections do not include any prohibition on espionage. The Paris Convention for the Protection of Industrial Property of 1883 governs international patterns and trademarks and particularly Article 10 foresees that Member states should guarantee national protection against unfair competition (Ziolkowski, 2013, p. 435). However, it does not include any interpretation on unfair competition in case of espionage operations and does not include any prohibition on economic espionage.

Another international document related to property rights protections is the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1994. The TRIPS Agreement has a broad scope because it covers both industrial and intellectual property and related rights which are at the heart of international economic relations in the scope of the World Trade Organization (WTO) (Ziolkowski, 2013). The basic purpose of the TRIPS Agreement is to

limit distortions and obstacles to international trade, to effectively and adequately protect intellectual and industrial property rights, as well as to ensure the measures and procedures to enforce these rights (Ziolkowski, 2013). Article 39(1) of the Agreement foresees an obligation to Member states to "*protect undisclosed information*" and "*data submitted to governments or government agencies*" (World Trade Organisation, 1994). In the same Article, there is a reference on "*honest commercial practices*" and in the footnote 10 there is a reference on "*breach of confidence*" but as Ziolkowski (2013) argues, there is not any reference on unlawful taking of proprietary information. Under TRIPS Agreement, every Member state has the obligation to protect information relating to intellectual property and industrial rights as well as trade secrets within their national territory, but there is not any prohibition on espionage operations against a foreign state, since the Agreement does not include any provisions on economic or industrial espionage on the international level (O'Hara, 2010).

The espionage operations of economic or industrial character that seek to acquire, in a clandestine manner, state information and secrets as well as information from private companies, have legal implications at the national level but there is no clear international prohibition of such operations. Overall, on the inter-state level regarding either traditional espionage or cyber, industrial and economic means, the policy that states follow is the policy of silence (Ziolkowski, 2013). states do not regularly make clear and sound their protests when they fall victim to espionage, except for incidents that include diplomatic staff, when the expulsion of diplomats follows from the target state. There is clear penalisation of espionage operations of every character in national law, but in times of peace, states have opted not to clearly regulate espionage operations, since espionage has been established as a widespread practice in international relations since the ancient times. This study will continue with the examination of modern cases of espionage internationally and will provide arguments in the case of regulating peacetime espionage.

## Modern cases of espionage

Espionage operations happen regularly without the public being aware of such operations. However, the most recent case came to light at the end of July in Greece, after the opposition leader of PASOK-Kinal and MEP of the S&D party, Nikos Androulakis, made public that he had filed a lawsuit with the Prosecutor's Office of the Supreme Court that there has been an illegal attempt to hack and tap his phone using the commercial Predator spyware on 21 September 2021 (Mildebrath, 2022). This act of espionage was revealed after an aide to Nikos Androulakis suggested that he gives his old phone to upgrade for a new one to the new spyware detection lab in Brussels at the European Parliament, where technicians found that he was the victim of a cyberattack in September 2021 with this malware called Predator (Horowitz & Kitsantonis, 2022). Predator spyware is manufactured by Cytrox, a technology company that operates from Greece and in the case of its installation through clicking on a phishing link, it can infect the entire cell phone, allowing thus the operators to monitor every aspect of a phone's features such as calls, messages, photos and videos (Mildebrath, 2022).

Concerning interception malware systems, it has to be underlined that according to reports from different Greek news outlets, in 2020 the National Intelligence Agency intended to purchase technology that would enable it to map internet communication, like traditional telecommunications, but Greek government's officials have rejected such rumours

(Mildebrath, 2022). Regarding this issue, it should be mentioned that opposition party leader and MEP Nikos Androulakis was not the only target of this Predator spyware. The revelations about Nikos Androulakis's case emerged only several days after the National Transparency Authority (EAD) had cleared the government in its investigations over the case of surveillance of a financial journalist named Thanasis Koukakis, who is known for his investigation of major Greek banks and banking figures (Mildebrath, 2022). Back in June 2020, the Greek national intelligence agency (EYP) had tapped both his phones, intercepting his communications from June to August 2020 on the grounds of national security and with authorisation from the in-house public prosecutor named Vasiliki Vlachou (Mildebrath, 2022; Clapp, 2022). Koukakis made an official complaint to Greece's watchdog of communication and privacy, the Hellenic Authority for Communication Security and Privacy (ADAE), but before getting an answer, the Greek government amended a law in March 2021, which allows it to withhold information from individuals for whom there are open investigations on the grounds of national security (Clapp, 2022). Although this Greek Authority claimed that it did not possess any information on his case, an investigation conducted by the news outlet, Reports United, which included state intelligence documents and the prosecutor's clear orders, revealed that the Greek National Intelligence Services indeed intercepted Koukakis's communications from June to August 2020 and showed that the state surveillance of the journalist ended the very same day he submitted his official complaint with Greece's privacy and communications watchdog (ADAE) (Mildebrath, 2022). However, in July 2021, he received a message in his phone with a phishing link, which he clicked on, resulting to the infection of his phone with the Predator spyware, which was discovered in March 2022 only after Citizen Lab, the world's distinguished experts on spyware, proceeded to test his device (Horowitz & Katsantonis, 2022). Following these events, the Greek government denied any engagement with this case.

Cybersecurity experts from Citizen Lab and Google have argued that actors purchasing spyware such as the Predator can be also governmental (Mildebrath, 2022). Despite journalists trying to establish links between spyware companies and governmental agencies, the National Transparency Agency (EAD) in Greece cleared the government in its investigations about the case of journalist Koukakis for the surveillance activities of the National Intelligence agency for the period June-August 2020 (Mildebrath, 2022). However, in a closed-door hearing on 29 July 2022, EYP Chief, Panagiotis Kontoleon, confirmed to the Committee on Institutions and Transparency of the Greek Parliament that the Agency had conducted a surveillance operation of Koukakis (Mildebrath, 2022). Despite the extent and the importance regarding the legality of such an espionage operation, the case of Koukakis did not receive the nation and Europe-wide attention that the case of Androulakis attracted. In his case, the Hellenic Authority for Communication Security and Privacy confirmed in early August that his phone was tapped by the National Intelligence Agency with the formal authorisation of the public prosecutor Vasiliki Vlachou (Mildebrath, 2022).

After the revelations on the case of Nikos Androulakis, former EYP Director, Panagiotis Kontoleon stated that the surveillance of Androulakis occurred after requests submitted from the intelligence services of both Ukraine and Armenia, but the Greek government denied these leaks and both countries rejected any involvement in this case (Mildebrath, 2022). On 5 August 2022, both the Chief of EYP, Panagiotis Kontoleon and the Secretary General to the Prime Minister, Grigoris Dimitriadis, resigned (Kathimerini, 2022; Naftemporiki, 2022). The first one resigned after mishandling the issue in lawful wiretapping operations according to him and

Dimitriadis assumed the political responsibility of this operation by resigning (Mildebrath, 2022). At this point it has to be noted that one of Prime Minister's Mitsotakis first acts when he was elected in July 2019 was to put the Greek National Intelligence Agency under his direct control (Clapp, 2022), but after the revelations occurred about the case of Nikos Androulakis, on 8 August 2022 he claimed that EYP indeed had tapped the phone of Nikos Androulakis, but did not comment on the reasons behind it and denied any previous acknowledgement of this operation, despite being responsible for supervising EYP (Mildebrath, 2022). Giorgos Gerapetritis, one of Mr Mitsotakis' closest aides at the government, he stated that he attempted to set up a meeting between the Director of EYP and Mr Androulakis, so that the chief of the Agency could explain him personally, as was permitted by law, the reasons he was put under surveillance, but it did not happen (Horowitz & Katsantonis, 2022).

In his statements over this case, Prime Minister Mitsotakis refrained from commenting directly on the connection between the Predator spyware and the phone tapping case and left many questions open. Instead of responding if Greece has acquired spyware systems such as Predator, he referred to proposals and interventions on four areas of EYP framework (Mildebrath, 2022). Moreover, he underlined a possible connection between this case and 'dark forces' outside of the country in order to destabilise the country and this possible involvement of foreign powers could be a threat to the common cause against Russia (Horowitz & Katsantonis, 2022). The statements of the Greek Prime Minister did not convince the opposition parties, which claimed that the government lied in order to avoid the fact that it was spying on its own citizens and political rivals (Horowitz & Katsantonis, 2022). The Greek government on the following day of Prime Minister's statements over the eavesdropping case, on 9 of August 2022, introduced an Act of Legislative Content, which reinstates two-prosecutor authorisation for surveillance operations as well as determines the formulation of an opinion from the competent parliamentary committee as mandatory in order to appoint every EYP Director (Mildebrath, 2022). The new Head of EYP was appointed following the new rule. However, transparency is still at stake when it comes to phone surveillance, as it does not repeal the March 2021 decision that prevents the state's privacy and communications watchdog, ADAE, from informing surveillance targets on surveillance measures undertaken in terms of national security (Mildebrath, 2022). On this matter, ADAE has argued that the March 2021 decision violates the guaranteed right to protection of confidentiality and privacy foreseen in the Constitution of the Hellenic Republic (Mildebrath, 2022).

Furthermore, in the case, the Greek Parliament attempted to address the act of espionage in various institutional settings. On 6 September 2022, the special parliamentary committee on inquiry commenced its work to deliver its conclusions on the case within a month. Regarding the case, various prosecutors have started to conduct investigations into both the Koukakis and Androulakis cases, while ADAE decided to visit the EYP premises to request relevant files on the cases (Mildebrath, 2022). However, the new EYP Director stated that the file on Androulakis's surveillance might have been erased, but according to the law, this should not happen before December 2023 (Mildebrath, 2022).

Considering the extent of such espionage operations, both cases of surveillance have caused political upheaval in Greece, pending parliamentary elections in the next summer. The scandal adds to the current European moment, considering that there have been spying operations in Spain, Hungary, Poland and France against journalists and opposition politicians as well as top EU officials (Clapp, 2022; Milderbrath, 2022). Although the opposition is demanding justice,

transparency and clarity on the cases, the Greek government currently insists on acknowledging certain facts about surveillance operations, insists on their legality, but repeatedly has rejected any involvement in purchasing or using the Predator spyware (Mildebrath, 2022). The examination of both cases is in progress and the details analysed are valid at the time of conducting this research. Taking into consideration such recent and relevant examples of espionage operations, it is essential to see this case study both due to the importance of the management of such an operation from a member state of the EU and the re-emergence of espionage in the political agenda of member states that will enhance the debate for the EU's possible attempts of regulating espionage in European law.

Other contemporary cases of espionage include the revelations from Snowden of NSA's surveillance activities of US citizens in 2013, abandoning constitutional safeguards on the collection of information on innocent US citizens, which raised important questions on the spying operations made by the NSA (Blusiewicz, 2014). Moreover, the US government and particularly the US Department of Justice, opened a case against him, with the charges of violating the Espionage Act of 1917 and stealing government property (Blusiewicz, 2014). Internationally, Snowden has been applauded for his bravery to bring such acts of unathorised surveillance into light, while US government officials have talked about treason, irresponsibility of unveiling illegally governmental operations as well as seeking asylum from one of the main rivals of US, namely the Russian federation, where it is rumoured that he still lives. Many operations have been unveiled internationally about espionage either from state or non-state actors and will continue to be unveiled in the future, but it should be considered that there are still operations that have not come to light and probably will never be revealed that pose a threat to both state security and privacy of citizens.

## Should regulating espionage be considered in international relations?

As it has been thoroughly analysed in the text, espionage is a complicated phenomenon regarding its legality or illegality during peacetime and is not regulated in international law, while it is not illegal according to international humanitarian law. All states prohibit acts of espionage that cause harm in their national interests under domestic law, but they have always practiced covert surveillance on both individuals and other foreign states. In peacetime, there is no treaty that explicitly permits espionage and regarding the arguments on its legality under the customary international law, there should be sufficient state practise and this should be supported by *opinio juris*, meaning that States have attempted to provide justifications for their actions by invoking international law, which is missing though in the case of espionage (Terry, 2015, p. 183). In case that spies of a state are caught in another State and are accused of espionage, they are not protected by any provision of international law during peacetime and states never claim that the conduct was legal and regularly follow either the policy of silence or denial. Moreover, on this matter, Chesterman (2006) has stated that "*state practice and opinio juris appear to run in opposite directions*" and argued about a disjuncture between sufficient practice of espionage by states and penalisation of espionage under domestic law (p. 1072). Despite states regularly conducting espionage operations, the lack of *opinio juris* does not conclude the legality of the practise of espionage.

Espionage has existed since ancient times and states have never stopped to practise it because either it is permitted because it is not forbidden or it is not regulated clearly, therefore not

justiciable under international law (Ziolkowski, 2013, p. 462). Due to the fact that the international system is anarchic, without a global government that sets the rule of behaviour and conduct, states themselves should fight for their own survival and espionage is a critical means to protect their national interests and national security. Earlier in the text, arguments have been analysed over the functional benefits of espionage, which is the increase of international ability and avoidance of war. However, there have been numerous times when states have manipulated or overestimated intelligence in order to justify debatable wars and interventions such as the attack in Iraq in 2003 (Terry, 2015). Moreover, the arguments over the right of self-defence under 51 of the UN Charter to justify the legality of espionage is largely unconvincing, considering that great powers tend to conduct espionage before an armed attack takes place in order to be better prepared.

At this point it should be noted that the nature of espionage has rapidly changed and this change remains an ongoing process. Espionage operations are not conducted anymore only by spies sent from a state to another state to attempt to steal information in a clandestine manner, but also remotely, through cyber means and satellites that have the capacity to inflict greater harm to opponents of a state in comparison with traditional espionage. Nowadays, this type of espionage is raising greater legal issues and poses a challenge to states in order to regulate espionage, either partly or fully. However, the regulation of espionage in international law is not an easy task. states consider espionage as a critical tool of their foreign policy and security policy and it is a common practice, either legal or illegal, in international politics. Moreover, states tend to find ways to conduct espionage without the target state being aware, such as the designation of a state's secret agents as diplomats and their inclusion to the diplomatic roster at an embassy to a foreign State. If spies, posing as diplomats, are caught performing espionage, according to the 1963 Vienna Convention, they are declared personae non gratae by the host state and expelled from the country (Radsan, 2007, p. 621). Moreover, the diplomatic immunity that comes along with the diplomatic status, does not legalise the practice of espionage, but protects the spies-diplomats from the domestic laws of the host country in case they are not caught. Spies that are included in the diplomatic roster of a country's embassy in a foreign state is a common practice in the field of international espionage, but the host state's intelligence services tend to consider every diplomat as a potential spy (Radsan, 2007, 621-622).

Considering what has been argued, international law cannot remain inert and oblivious on the question of regulation of espionage. The new developments and rapid changes in the field of technology enhance the power of cyber espionage, which is a threat that the world has not possibly seen its highest potential yet. In response to foreign cyber espionage, many states have attempted to adapt their national cyber security strategies and employ diplomatic, economic and political means to thwart the rapid development of cyber espionage. Despite the great danger that accompanies espionage, even with the growing development of cyber means, it is illusionary to believe that states will clearly regulate espionage and outlaw it, as they would never deprive themselves of such a longstanding tool in their foreign policy agenda.

## Conclusions

This study observed that espionage is allowed in international humanitarian law or law of war, which also determines the treatment and the rights of spies in case of their capture. Although espionage in war is not illegal under IHL and does not create grounds for complaint between

states under international law, IHL does not offer adequate legal protection to war spies captured in the act (Beck, 2011, p. 2011). In case a spy is caught, he is subject to the laws of the domestic criminal law, but he is not punished without a fair trial, and his return to friendly forces grants him "immunity" for past actions if he is later caught. It is necessary for the persons that are engaging in espionage to wear the uniform of their armed forces in order not to be considered and treated as spies. Spies in wartime, either civilians or military, caught in the act of espionage, are not entitled to the prisoner of war status, unless they are soldiers in uniform. Unlike soldiers in uniform, the other individuals cannot claim the right to a prisoner of war status, therefore it should be clearly stated that the principle of distinction constitutes the legal foundation, in international law, in order to be treated as a prisoner of war. Although espionage is clearly regulated during wartime in international law, particularly in international humanitarian law, there is less consensus as to peacetime espionage.

In peacetime, states tend to conduct espionage against other states merely for reasons of self-defence and for their own interests, which can be of economic, security, industrial or cyber character. This can be explained from the fact that there is neither a treaty nor a customary international rule that clearly and explicitly prohibits espionage, therefore it is not possible to argue that espionage is illegal as Baker (2003) has also claimed. In peacetime, spies are not protected by any treaty and thus the country that captured them has the right to imprison them according to its domestic criminal law. An exception exists regarding the diplomatic staff of a country's embassy, which in case of spying at the territory of another state, they are designated as 'personae non gratae' and expelled from the country.

On peacetime espionage, it has been argued that there are three different strands of thought. There are scholars and other commentators claiming that peacetime espionage is legal, arguing either about its functional value in improving cooperation or as a means of peremptory self-defence under the UN Charter and international law, serving as a form of both arms control and conflict prevention. Moreover, there are scholars talking about the establishment of customary norms for the permissibility of peacetime espionage due to its historical acceptance and widespread practice in the passage of time, thus indirectly implying legality under international customary law.

Regarding the illegality of peacetime espionage, the main arguments are based on the non-interference and non-intervention principle as well as the protection provided for the territorial integrity and sovereignty of a state by the UN Charter and other international treaties and this study analysed cases that have depicted in practice such protections. Meanwhile, there are human rights treaties that refer to individual rights such as the right to privacy that are threatened from possible espionage activities. Last but not least, diplomacy and espionage have gone hand in hand many centuries now, so there are also legal treaties that refer to the restrictions and repercussions of any espionage activities conducted by a foreign state's officials and embassy against the host state.

Last but not least, another strand of arguments on peacetime espionage is based on the view that espionage is neither legal nor illegal. Baker (2003) points out the functional benefits of espionage in enhancing international cooperation to have a united response from states towards international issues such as terrorism, human trafficking, illegal migration and health

challenges. On this point of view, it has also been argued that espionage creates functional benefits for the international community, considering that a possible exchange of intelligence among states would drive the development of international norms and strengthen global security (Chesterman, 2006).

Espionage has been a longstanding state practice to acquire clandestinely important intelligence from another State and the use of spies has been a calculated risk in case of capture. In the passage of time and especially in the 21st century, the nature of espionage operations has rapidly changed and evolved due to the technological advancements, providing a unique opportunity to state or non-state actors to not only acquire large-scale information from another state, but also to generate possibly greater damage than the traditional espionage, as cyber espionage offers new opportunities and possibilities in terms of ease, speed and inexpensiveness of intelligence collection. Moreover, a great advantage of cyber espionage is that it can be conducted both remotely and anonymously, a challenge that makes states vulnerable to such attacks, which are gradually enhancing and adapting their cyber security capabilities to deal with the new challenges that the cyber era brings.

Cyber espionage is not the only challenge in the new era, as incidents of both economic and industrial espionage are increasing, with both state and non-state actors engaging with these forms of espionage to safeguard their own national or business interests. Despite the fact that such actions have legal implications at the national level, there is no clear international prohibition of such operations. Overall, on the inter-state level regarding either traditional espionage or cyber, industrial and economic means, the policy that states follow is the policy of silence or denial when they are the perpetrators, but they choose the policy of protest in case they fall victims to such espionage actions. Probably, the most controversial and unclear element of espionage, which remains open to international law and whose interpretation is the subject of further study, is that of cyber operations and the acquisition of processed information in cyberspace. Whether states will continue to evolve their conception of state sovereignty extending beyond physical borders to the remote and virtual acquisition of information, and whether this evolution is possible in an age of ongoing development of technology, are matters to consider when we attempt to project international law into the future.

The art of spying has a peculiar dual identity as Pun (2017) argues. While states openly admit the existence of their own intelligence agencies and claim their espionage activities as legitimate and necessary to safeguard national security, they also aggressively condemn foreign espionage and consider any domestic support of foreign espionage as a crime. Prosecution or the threat of prosecution of spies by a target state under its own domestic laws should not be considered as an assertion that the practice as such is a violation of international law. Considering the fact that most states conduct such activities themselves, it may more properly be viewed as an effort to deny information to foreign states or increase the costs of doing so in an effective manner. Chesterman (2006) argues that these inconsistencies have led commentators and theorists to claim that the issue of addressing the legality of intelligence gathering under international law as oxymoronic.

Furthermore, states have intentionally opted not to clearly regulate espionage operations, since espionage has been established as a widespread practice in international relations since the ancient times and is considered as an essential instrument to safeguard their national interests and security in the anarchic international community. Despite the great danger that accompanies espionage, even with the growing development of cyber means, it is illusionary to believe that states will clearly regulate espionage and outlaw it, as they would never deprive themselves of such a longstanding tool in their foreign policy agenda.

There are provisions in international humanitarian law or law of war regarding the legality of espionage and the treatment of spies, but in peacetime such provisions either are not clear or do not exist. states would never proceed to clear regulation of espionage in international law and therefore have clear prohibition of acts of espionage. Espionage and intelligence collection will probably continue to exist as a necessary practice as states are capable of securing specific national interests in this debatable, in legal terms, way. Spies will continue to be employed for a country's interests, including the risk of being captured and not protected by either their own country of origin or by international law regulations. However, considering what has been argued in this study, international law cannot remain inactive and oblivious to the question of regulation of espionage. The new developments and rapid changes in the field of technology enhance the power of cyber espionage, which is a threat that the world has not possibly seen its highest potential yet. In response to foreign cyber espionage, many states have attempted to adapt their national cyber security strategies and employ diplomatic, economic and political means to thwart the rapid development of cyber espionage.

Despite the fact that espionage is a 'necessary evil', a possible regulation of espionage is still a field of research that needs to be tackled and developed more in academic bibliography. This study has attempted to address the challenging issue of the international legal perspectives on espionage, in both peacetime and wartime, shedding light into the different arguments on the legality or illegality of espionage and how the new forms of espionage could trigger a possible regulation of espionage in international law. One of the limitations of this proposed research is that there is insufficient academic literature on the subject. As this area is under-researched and under-developed in the field of international relations, there is a limited bibliography. Therefore, this thesis attempts to provide insights on the international legal perspectives on espionage, expand on the current literature, as well as further the academic debate on such an interesting dimension of international affairs and politics.

## Reference List

### Foreign sources

Adams, M. J. (2014). Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace. *Harvard National Security Journal*, *5*, 377-460.

Anderson, D. A. (1990). Spying in violation of Article 106, UCMJ: The offense and the constitutionality of its mandatory death penalty. *Military Law Review*, *127*, 1-61.

Andrew, C. & Dilks, D. (1984). *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. University of Illinois Press.

Baker, C. D. (2004). Tolerance of International Espionage: A Functional Approach. *American University of International Law Review*, *19*(5), 1091-1113.

Beck, N. J. (2011). Espionage and the Law of War. *American Intelligence Journal*, *29*(1), 126-136.

Beim, J. (2017). Enforcing a prohibition on international espionage. *Chicago Journal of International Law*, *18*(2), 647-672.

Blusiewicz, J. (2014). The Case of Edward Snowden: A Different Path. *Cornell International Affairs Review*, *8*(1).

Boadle, A. (2013, September 9). *NSA spying on Petrobras, if proven, is industrial espionage: Rousseff*. Reuters. Retrieved September 8, 2022, from https://www.reuters.com/article/us-usa-security-snowden-petrobras/nsa-spying-on-petrobras-if-proven-is-industrial-espionage-rousseff-idUSBRE98817N20130909

Burn, M. (1970). *The Debatable land: a study of the motives of spies in two ages*. Hamish Hamilton.

Cambridge Dictionary. (n.d.). Spy. In *Cambridge Dictionary*. Retrieved August 10, 2022 from https://dictionary.cambridge.org/dictionary/english/spy

*Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June, 1986, https://www.refworld.org/cases,ICJ,4023a44d2.html

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html [accessed 9 October 2022]

Central Intelligence Agency (Office of Public Affairs). (1999). *A consumer's guide to intelligence: gaining knowledge and foreknowledge of the world around us*. National Technical Information Service.

Chesterman, S. (2006). The Spy Who Came in from the Cold War: Intelligence and International Law. *Michigan Journal of International Law, 27*(4), 1071-1130.

Clapp, A. (2022, August 22). *The rot at the heart of Greece is now clear for everyone to see*. The New York Times. Retrieved September 21, 2022, from https://www.nytimes.com/2022/08/22/opinion/greece-mitsotakis-predator-spyware.html

Convention on International Civil Aviation (Chicago Convention), 7 December, 1944, https://www.icao.int/publications/pages/doc7300.aspx

Crowdy, T. (2007). *Ιστορία της Κατασκοπείας*. [The Enemy Within: A History of Espionage]. Athens: Lector Publications.

Deeks, A. S. (2016). Confronting and adapting: Intelligence agencies and international law. *Virginia Law Review*, *102*(3), 599-685.

Demarest, G. B. (1996). Espionage in International law. *Denver Journal of International Law and Policy*, *24*(2), 321-348.

Espionage. (n.d.). In *West's Encyclopedia of American Law, edition 2*. (2008). Retrieved from: https://legal-dictionary.thefreedictionary.com/Espionage

European Union, European Union Agency For Cybersecurity (ENISA). (2020). *Cyber espionage* (ENISA Threat Landscape). https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-cyberespionage

Falk, R. (1962). Space Espionage and World Order: A Consideration of the Samos-Midas Program. In R.J. Stranger (ed.). *Essays on Espionage and International Law* (46-82). Ohio State University Press,

Fleck, D. (2007). Individual and State Responsibility for Intelligence Gathering. *Michigan Journal of International Law, 28*(3), 687-705

Forcese, C. (2016). Pragmatism and Principle: Intelligence Agencies and International Law. *Virginia Law Review*, *102*, 67-84.

Gardner, J. G. (1965). General Order 100 Revisited. *Military Law Review*, *27*, 1-48.

Garner, B. A., & Black, H. C. (2009). *Black's law dictionary*. 9th ed. West.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=AE2D398352C5B028C12563CD002D6B5C

Griffith, S. B. (1971). *The art of war*. Oxford University Press.

Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, https://ihl-

databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8

Haider, H. (2013). *International legal frameworks for humanitarian action: Topic guide.* GSDRC, University of Birmingham.

Hastings, M. (2016). *Spies, Codes and Guerrillas 1939-1945*. William Collins.

Horowitz, J., & Kitsantonis, N. (2022, August 12). *A Greek scandal reverberates as eavesdropping expands in Europe*. The New York Times. Retrieved September 18, 2022, from https://www.nytimes.com/2022/08/12/world/europe/greece-surveillance-europe-kyriakos-mitsotakis.html

Instructions for the Government of Armies of the United States in the Field (Lieber Code), 24 April 1863, https://ihl-databases.icrc.org/ihl/INTRO/110

Intelligence. (1960). In *Dictionary Of The United States Military Terms For Joint Usage*. Retrieved from: https://archive.org/details/DictionaryOfTheUnitedStatesMilitaryTermsForJointUsage/mode/2up

Jennings, R., & Watts, A. (1992). *Oppenheim's international law peace* (9th ed.). Longman.

Kelsey, F. W. (1925). Hugo Grotius: The law of war and peace. *The Classics of International Law*. Clarendon Press.

King James Bible. (2008). Oxford University Press. (Original work published 1769)

Kish, J. (1995). *International law and espionage*. Martinus Nijhoff Publishers.

Konstantopoulos, I. L. (2010b). *Macroeconomic Espionage: Incentives and Disincentives*. Research Institute for European and American Studies.

Lerner, K., & Lerner, B. (2004). In *Encyclopedia of espionage, intelligence, and security* (A-E, Vol. 1). Gale.

Lin, H. S. (2010). Offensive cyber operations and the use of force. Journal of National Security Law and Policy, *4*(1), 63-86.

Lipton, E., Sanger, D. E., & Shane, S. (2016, December 13). *The perfect weapon: How russian cyberpower invaded the U.S.* The New York Times. Retrieved September 8, 2022, from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Lubin, A. (2016). Espionage as a Sovereign Right under International Law and its Limits. I*LSA Quarterly*, *24*(3), 22-28.

Maras, H, M. (2016). *Cybercriminology*. Oxford University Press.

MI5. (n.d.). *Counter-Espionage*. https://www.mi5.gov.uk/counter-espionage

Mildebrath, H. (2022). *Greece's Predatorgate - The latest chapter in Europe's spyware scandal?* European Parliamentary Research Service. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

O'Hara, G. (2010). Cyber-Espionage: A Growing Threat to the American Economy. *CommLaw Conspectus: Journal of Communications Law and Technology Policy*, *19*(1), 241-275.

Olson, J. M. (2006). *Fair play: the moral dilemmas of spying*. Potomac Books, Inc.

Omand, D. (2015). Understanding Digital Intelligence and the Norms That Might Govern It. *Global Commission on Internet Governance, 8,* 1-19.

Pelican, L. (2012). Peacetime Cyber-Espionage: A dangerous but necessary game. *CommLaw Conspectus: Journal of Communications Law and Technology Policy. 20.* 363-390

Porteous, S. (1995). Economic/Commercial Interests and the World's Intelligence Services: A Canadian Perspective. *International Journal of Intelligence and Counterintelligence, 8,* (3), *275-306.*

Project of an International Declaration concerning the Laws and Customs of War (Brussels Declaration), Brussels, 27 August 1874, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=42F78058BABF9C51C12563CD002D6659

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/4e473c7bc8854f2ec12563f60039c738/2a0b6343a399db8ac12563cd0051dc0d

Pun, D. (2017). Rethinking espionage in the modern era. *Chicago Journal of International Law*, *18*(1), 353-391.

Radsan, A. J. (2007). The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law*, *28*(3), 596-623.

Random, A. (1958). Intelligence as a science, *CIA Studies in Intelligence, 2,* 75-79.

Risen, T. (2013, September 24). *Brazil's president tells U.N. that NSA spying violates human rights*. U.S. News. Retrieved September 8, 2022, from https://www.usnews.com/news/articles/2013/09/24/brazils-president-tells-un-that-nsa-spying-violates-human-rights

Sanchez, J. E. (2017). Intelligence Collection, Covert Operations, and International Law. *The Intelligencer. 23*(1). 73-78

Schaller, C. (2013). Spies. *Max Planck Encyclopedia of Public International Law*.

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Scott, D. R. (1999). Territorially Intrusive Intelligence Collection and International Law. *Air Force Review*, *46*, 217-226.

Silver, D. B. (2005). Intelligence and counterintelligence. *National Security Law*, *2*, 935-965.

Stone, J. (1962) Legal Problems of Espionage in Conditions of Modern Conflict. In R. J. Stanger (ed.). *Essays on Espionage and International Law* (pp. 29-43). Ohio State University Press,

Terry, P. (2015). "Absolute Friends": United States Espionage Against Germany and Public International Law. *Revue québécoise de droit international/Quebec Journal of International Law/Revista quebequense de derecho internacional*, *28*(2), 173-203.

The International Committee of the Red Cross's Advisory Service on IHL. (2022, April 7). *What is international humanitarian law?* International Committee of the Red Cross. Retrieved August 8, 2022, from https://www.icrc.org/en/document/what-international-humanitarian-law

The Laws of War on Land, 9 September 1880, https://ihl-databases.icrc.org/ihl/INTRO/140?OpenDocument

UN General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, https://digitallibrary.un.org/record/202170?ln=en

United Nations Security Council, *Security Council resolution 138 (1960) [Question relating to the case of Adolf Eichmann]*, 23 June 1960, https://www.refworld.org/docid/3b00f1cc74.htm l

United Nations, *Charter of the United Nations*, 24 October 1945, https://www.refworld.org/docid/3ae6b3930.html

United Nations, United Nations Convention on the Law of the Sea, 10 December 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Vienna Convention on Diplomatic Relations, 18 April 1961, https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

von Bogdandy, A. & Rau, M. (2006). The Lotus. *The Max Planck Encyclopedia of Public International Law.*

World Trade Organisation. *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)*, 15 April 1994, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf

Wright, Q. (1962) Espionage and the Doctrine of Non-Intervention in Internal Affairs. In R. J. Stanger (ed.). *Essays on Espionage and International Law* (pp. 3-28). Ohio State University Press.

Ziolkowski, K. (2013). Peacetime cyber espionage–new tendencies in public international law. In Ziolkowski (Ed.), *Peacetime Regime for State Activities Cyberspace, International Law, International Relations and Diplomacy* (pp. 425-464). NATO CCD COE Publication.

**Greek Sources:**

Gerolymatos, A. (2001). *Κατασκοπεία στην Αρχαία Ελλάδα*. [Espionage in Ancient Greece]. Athens: Cactus Editions

Hadjikonstantinou, K. (2009). *Προσεγγίσεις στο Διεθνές Ανθρωπιστικό Δίκαιο.* [Approaches to International Humanitarian Law]. Athens: Ioannis Sideris Publications.

Koliopoulos, K. (2008). *Η στρατηγική Σκέψη Από την αρχαιότητα μέχρι σήμερα.* [Strategic thinking From antiquity until today]. Athens: Poiotita

Konstantopoulos, I. L. (2010a). *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη.* [Economy and Espionage. Theory and Practice]. Athens: Poiotita

Newsroom. (2022, August 5). Παραιτήθηκε ο διοικητής της ΕΥΠ, Παναγιώτης Κοντολέων – στη θέση του ο Θεμιστοκλής Δεμίρης [The head of the EYP, Panagiotis Kontoleon, has resigned - Themistoklis Demiris has been appointed in his place] *Η ΚΑΘΗΜΕΡΙΝΗ* [KATHIMERINI]. Retrieved September 21, 2022, from https://www.kathimerini.gr/politics/561988267/paraitithike-o-dioikitis-tis-eyp-panagiotis-kontoleon-sti-thesi-toy-o-themistoklis-d emiris/

Vasileiadis, P. (2018). *Η κατασκοπεία στο Διεθνές Δίκαιο*. [Espionage in International Law]. Athens: Sakkoula Publications.

Vrionis, K. (1960). *Η Κατασκοπεία ως Νόμιμον Στρατήγημα Πολέμου και ως Αξιόποινον Στρατηγικόν Μέσον κατά της Εθνικής Αμύνης της Πολιτείας (Συμβολή εις την Θεωρίαν του Ποινικού Δικαίου).* [Espionage as a Legal Stratagem of War and as a Valuable Strategic Means against the National Defense of the State (Contribution to the Theory of Criminal Law]. Athens: Athenae

*Παραιτήθηκε ο Γρηγόρης Δημητριάδης, γενικός γραμματέας του πρωθυπουργού* [Grigoris Dimitriadis, secretary general to the prime minister, resigned]. (2022, August 5). naftemporiki.gr. Retrieved September 21, 2022, from https://naftemporiki.gr/story/1893111/paraitithike-o-grigoris-dimitriadis-genikos-grammateas-tou-prothupourgou

## Annex

It has been argued that espionage is regulated and allowed in International Humanitarian Law (IHL) and ruses of war are permitted in the context of a war or an armed conflict. However, this is not the case during peacetime at the international level. At the international level, espionage is 'tolerated' since there is no official international legislation to prohibit espionage actions. Espionage is considered a covert activity and an exceptional tool to obtain clandestinely classified information from a foreign state or private entity, either through the use of agents or cyber means in order to provide better and well-informed decision-making to policy makers of an enemy state. It has been established as a widespread practice in international relations since ancient times. However, at a national level, states have indicated that there are two ways to deal with foreign espionage and foreign agents. The first one is counterespionage, which is both defensive and offensive, as a State does not aim exclusively to deal with the protection of its information and interests from foreign agents and espionage actions, but also try to gain information for its enemies and obtain critical information about its capacities at any level, such as political, military or financial. The second method is the establishment of legal regulations in their domestic criminal law and in Military Manuals or Military Penal Codes. At the end of the 19th century, in order to deal with spies, to protect classified information and by extension the national interests of each state, governments had to legislate in such a way as to prevent them as well as punish the captured spies in regular trials for their criminal actions, as espionage is considered in criminal action in the domestic criminal law of the majority of states worldwide.

In the US, for instance, the Espionage Act is a federal law passed in 1917, shortly after the US entered World War I, with the goal to deal with wartime activities designated as dangerous or disloyal, including attempts to acquire defence-related information with the intent to inflict harm to the United States, or obtain code and signal books, photographs, or other such documents to communicate them with the US's enemies (Office of the Director of National Intelligence, n.d.). The Act also outlawed false statements with the intent to interfere with military operations, attempts to provoke insubordination or obstruct the recruitment of troops as well as false statements supporting the success of the US's enemies (Office of the Director of National Intelligence, n.d.). The individuals captured and charged with violations were entitled to a $10,000 fine and twenty years imprisonment, but in case the crimes were committed during wartime, the punishment could be thirty years imprisonment or even the death penalty (Office of the Director of National Intelligence, n.d.). Espionage Act is still in force and many cases have been processed through the Act such as the case of Edward Snowden, who was charged with "*unauthorized communication of national defense information*" and "*willful communication of classified communications intelligence information to an unauthorized person*" under the Espionage Act after releasing in public documents about the NSA's PRISM surveillance program (Finn, P., & Horwitz, S., 2013).

Another example of an attempt of domestic legislation regulating espionage can be derived from the United Kingdom and its Official State Secrets Act established in 1889 (The National

Archives, 1989). The Official Secret States Act was followed by a series of Acts to revise it. Since then, several changes followed in 1920, 1939, 1989 with the last amendment to that of 1989 being established in 2007, which proves the effort to continuous modernization to deal with the current global challenges. The Official Secrets Acts 1911-1989 constitutes today the main legal regulation and protection in the UK against acts of espionage and unauthorised disclosure of official information (Bartlett, G., & Everett, M., 2017). The Official Secrets Act 1911 regulates offenses related to espionage, sabotage and related crimes, while the Official Secrets Act 1989 foresees the offenses connected with the unlawful disclosure of official information in six separate categories by employees of the UK's Government. It was established as an Act to prevent the Disclosure of Official Documents and Information. For actions of espionage, the maximum term of imprisonment according to the Official Secrets Act 1911 (as amended by the Official Secrets Act 1920) is fourteen years, but longer sentences are applied to a series of offenses (Bartlett, G., & Everett, M., 2017).

Taking into consideration the aforementioned examples of attempts of regulation of espionage at the national level, it will continue to exist as an ambiguous, in legal terms, practice in international relations in peacetime. While espionage is regulated in International Humanitarian Law as a legal practice, States have intentionally not regulated the covert activity of espionage at the international level and in international law as it is an essential practise to safeguard their survival in the anarchic international system. As long as there are threats to international or national security that urge states to use covert action against each other in their foreign policy in order to obtain the necessary intelligence and have the relevant foreknowledge for their national security and take decisions accordingly to their own interests at various levels, espionage will remain a 'necessary evil' in international relations and a vague concept in international law during peacetime.

**Reference List**

Office of the Director of National Intelligence (n.d.). *The Espionage Act of 1917*. INTEL. Retrieved November 26, 2022, from https://www.intel.gov/evolution-of-espionage/world-war-1/america-declares-war/espionage-act

Finn, P., & Horwitz, S. (2013, June 21). *U.S. charges Snowden with espionage*. The Washington Post. Retrieved November 26, 2022, from https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

The National Archives. (1989, May 11). *Official Secrets Act 1989*. Legislation.gov.uk. Retrieved November 26, 2022, from https://www.legislation.gov.uk/ukpga/1989/6/contents

Bartlett, G., & Everett, M. (2017). *The Official Secrets Acts and Official Secrecy* (House of Commons Library Briefing Paper CBP07422). https://researchbriefings.files.parliament.uk/documents/CBP-7422/CBP-7422.pdf