Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

FROM ANCIENT ESPIONAGE TO CYBER WARFARE: EVOLVING THREATS AND THE NEED FOR MODERN LEGAL FRAMEWORKS

BAHA' ALDEEN RAED SULIMAN ALMOMANI

Faculty of Languages and Communication, Doctor of Philosophy, English Language Studies, University Sultan Zainal Abidin, Unisza. Email: Almomanibaha5@gmail.com, Safabaha2008@gmail.com, ORCID ID: 0009-0006-8383-1986.

Madya Dr. MOHD NAZRI BIN LATIFF AZMI

Supervisor, Professor, Faculty of Languages and Communication, University Sultan Zainal Abidin, Unisza, Malaysia. Email: mohdnazri@unisza.edu.my

Abstract

The ancient art of espionage has undergone significant modification. This is particularly true in the last few decades because of the rise of technology-assisted combat, which has altered what security means to a person or even a country. This study explores the trends in espionage usage over time and how traditional methods changed as a result of technical advancements, especially in information gathering. Existing legal systems are failing more and more as the danger to global order and sovereignty spreads to cyberspace. The study concludes by highlighting the combination of state-based approaches to cyberspace management and arguing that laws governing the conduct of cyberspace operations under specific circumstances are necessary to protect state integrity and promote international peace.

Keywords: Espionage, National Security, Cyber Espionage, International Law, Information Warfare.

INTRODUCTION

Espionage is an ancient practice, but modern society and its applications have deviated from the fundamental cause of its definition. Indeed, the evolution of the practice of espionage, especially with the emergence of cyber warfare, poses a threat to the current laws and principles both at the national and international levels with the need for resetting new stand-alone laws and systems to address such issues. According to historical literature, the beginning of spying goes back to the Biblical times of sending spies to spy on Jericho (Joshua 2:1-24). There are also, however, some spying-related stories in the Islamic Quran, more so about the reign of Solomon, who was referred to as Sulaiman, involving gathering intelligence and controlling birds and djinn to help him become a king and waging wars. For instance, a bird was sent as a spy on the people of Sheba which is considered as petty spying (Quran, 27:20-24). This particular story reveals so much about the interplay of strategies, power, and intelligence to accomplish an objective as a leader, offering a window to the craft of espionage that has existed for quite a while.

No less in the case of Ancient Greece, a historical period marked by constant clashes between city-states, the sending of spies to watch over the activities of foes was quite commonplace (Richmond, 1998). Espionage regarded by many, especially leaders, as one of the effective means of running and or keeping a state, has certainly developed from the rudimentary stages toward modern practices. The rudimentary forms of espionage were accepted and as Jeffery (2010a) points out, ancient Egyptian states

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

employed spies to monitor their adversaries. The discipline of espionage began to develop as a separate from military intelligence despite technological advancements. This transformation, especially at the tail end of the twentieth century, is very pronounced considering the establishment and interdependence of intelligence agencies as pointed out by Andrew (2018) for the better management of domestic threats in this era of globalism.

As a necessary aspect of insecurity management and preservation of the state, it has also transformed into a tool for security intelligence and strategy formulation and implementation as well as for military, political, and economic operations. Politics is also about getting information, as Huband (2013) shows in his book *Trading Secrets: Spies and Intelligence in an Age of Terror*. Such concepts as the ‘art of surprise’, which Huband argues, is paramount for political leaders, military generals, and spies clearly outline the importance of espionage in governance even in the contemporary world. In the modern world characterized by extreme growth in science and technology especially in the cyber sphere, modern espionage calls for a wide-ranging global legal regime that must be regulated. The ever-growing sophistication of cyber espionage especially from the aspect of non-state actors is also a threat to international peace and security thus calls for urgent legislative measures to address the safety of the state.

The practice of spying is one of the most necessary implements engaged in national security, affecting states’ political maneuvers and military operations. The historical and ethical aspects of espionage as justified by the need to safeguard the state’s interests suggest the continuous examination of espionage concerning its legal and ethical practices, especially during war. Huband (2013) examines espionage from a variety of angles in *Trading Secrets: Spies and Intelligence in an Age of Terror*, tying literary themes and military intelligence operations together. These themes are a reflection of how espionage has been viewed historically concerning strategic goals meant to achieve intelligence success. Neligan (1999), quoted by Huband, states that "espionage is one of the toughest games played." It is difficult to find an agent in the appropriate position, but once one is located, he should be treated as a priceless gem, much like a nice wife (Neligan, 1999, p. 83 as referenced in Huband, 2013, p. 34). This quotation emphasizes the strategic importance and high stakes of espionage, which is essential to accomplishing objectives related to national security.

In addition to sending moral messages about defending the state and its citizens, espionage is essential for bolstering national security. According to Keil (2023) in *A Very British Dictatorship: The Defence of the Realm Act in Britain*, 1914-1920, national espionage played a critical role during the war. When Britain entered the First World War, it did not have a recognized set of emergency powers, in contrast to other belligerents. However, the *Defence of the Realm Act* (DORA), which reflected the changing political and legal environment under pressure from war, gave the government the authority to suspend constitutional principles and rule by decree. Keil (2023) also highlights how emergency powers' function in preserving national security changed dramatically, especially after the 1917 Bolshevik Revolution. Ethical questions about civil liberties and

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

state power are still being discussed concerning DORA's use of intelligence services, surveillance, censorship, and incarceration without trial.

An examination of the history of espionage as well as its inclusion in national security policies indicates how difficult it is to maneuver between state safety and individual rights. The misuse of emergency powers in, for instance, wartime Britain demonstrates that while espionage operations are undertaken to protect the political and legal issues of a state, they can also be employed to undermine them. In the present day, it is imperative to revisit this perspective, particularly in light of new challenges such as cyber attempts by hostile foreign powers and the growing involvement of non-governmental entities in the intelligence realm.

Internment, which refers to the confinement of individuals based on enemy associations or the suspicion of spy activities, poses serious moral and ethical challenges in terms of state security. Combatants and enemy civilians dynamic and enmeshed in the conflict were distinguishable from enemy civilians under their protection. However, the concept of enemy aliens raised serious issues regarding civil rights and the legitimacy of such policies. During World War I, the problems of espionage, censorship, and surveillance caused secret agency employees to change their allegiances and sparked concerns about espionage infiltrations. According to Farney and Kordan (2005) in *The Predicament of Belonging: The Status of Enemy Aliens in Canada, 1914*, conscription had previously given legitimacy to the practice of holding foreigners in warring nations. Because of this, enemy immigrants were detained on suspicion of being spies dispatched by their home nations. Even if they were not physically engaged in warfare, civilians were also subject to this practice since they were frequently viewed as possible dangers because of their nationality. However, there was a distinct difference between hostile civilians and captured combatants. Except for reservists and merchant marines, who were regarded as combatants by international law, this distinction, as defined by international law, guaranteed that civilians would not be held as prisoners of war (Farney & Kordan, 2005). The detention of enemy aliens during the First World War is an illustration of the distortions in thinking about war and warfare that justify, in this case, the internment of a section of the population without trial. The line, or lack thereof, between combatants versus civilians, and the principles governing such relationships during peace and war raise crucial concerns regarding the extent to which state power can be exercised where national security is at stake. Such events have their historical, or rather contemporary pretty similar to the so-called anti-espionage measures of post 9/11 America.

The First World War in Canada saw the opposing treatment of immigrants and enemy nationals exemplifying the conflict between the need for national security and the respect for people`s freedoms. Furthermore, it shows how people who posed no real threat were targeted by the state to appease public concerns about possible spying activities. It was the colonial mentality of that period that brought about these prejudiced strategies which could not allow some immigrants to assimilate into the body politics and whose nationality or loyalty were branded as unpatriotic. Similarly, during the war, other nations, such as Canada, were battling the external dangers of espionage. To safeguard national security,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

authorities in Canada devised counter-espionage tactics to address border security issues, as detailed by Farney and Kordan (2005). They point out that out of fear of espionage, border guards firmly followed government directives that forbade enemy immigrants from departing, detaining hundreds of those who were trying to escape to safety. The populace, which was already unsettled by rumors of espionage and sabotage, grew even more so when the government issued more Orders-in-Council to increase the authority of local authorities and lessen perceived dangers.

The national origins of immigrants made it more difficult for Canada to welcome them because of its concern that people from hostile nations might commit espionage. According to Farney and Kordan (2005), Canada's imperialist perspective significantly influenced its policies during the conflict in two ways. First, the idea that non-British immigrants' allegiance resided with foreign governments was strengthened by the denial of complete political integration, particularly to those from hostile countries. Second, this colonial mentality helped to categorize these people as enemy combatants, which further supported their monitoring and exclusion.

The national origins of immigrants made it more difficult for Canada to welcome them because of its concern that people from hostile nations might commit espionage. According to Farney and Kordan (2005), Canada's imperialist perspective significantly influenced its policies during the conflict in two ways. First, the idea that non-British immigrants' allegiance resided with foreign governments was strengthened by the denial of complete political integration, particularly to those from hostile countries. Second, this colonial mentality helped to categorize these people as enemy combatants, which further supported their monitoring and exclusion. As a case study in the discriminatory practices of immigration that emphasize allegiance and loyalty over civil rights, the significance of Canada's treatment of enemy aliens and immigrants in wartime is framed within an imperialist ideology of national security. These policies, which were largely influenced by the fear of spies, proved to be especially significant to the development of the nation's laws and politics that exposed the intricacies of security and identity concerning state power politics.

Nation states all over the world use intelligence in one form or another all contributing to the vast body of literature on the subject, harking back to the British Imperial tradition of spying on and collecting intelligence about other nations. Nations are beginning to work out safeguards against the usurpation of individuals’ privacy and the mounting threats of surveillance. Espionage is vital for safeguarding the structure of international relations but when countries start relying too much on intelligence operations, ethical dilemmas begin to surface. The imperial background shows that the framework for contemporary espionage techniques was created by Britain's experience growing its empire, particularly through intelligence networks. According to McIndoe in *A Pluralistic Imperialism?: Britain’s Understanding of Sovereignty at the Signing of the Treaty of Waitangi* (2015), the growth of settler nations during the 19th century caused a change in how sovereignty was understood, emphasizing national autonomy as opposed to Britain's imperial dominance. As a result of this ideological change, colonial legislatures supported

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

assimilationist tactics against indigenous populations, while Britain recognized indigenous sovereignty in other territories. The larger trend toward defending national sovereignty as a way to fend off the expansionist impulses of imperial powers is exemplified by this change in political and legal thinking.

Many modern espionage techniques have their roots in Britain's lengthy history of intelligence operations, especially in Ireland. As noted by Huband (2013), Britain's historical use of spies had an impact on the intelligence community's creation of counter-espionage tactics, clandestine operations, and clandestine ties between enemies. In my opinion, espionage involves more than just obtaining information; it also entails fostering international ties and trust.

Even if this can result in partnerships that were previously unimaginable, there are still serious ethical issues with surveillance and invasion of privacy. The difficulty, both historically and currently, is striking a balance between protecting individual rights and moral principles and maintaining national security. The British Imperial Setup has forged how espionage came to be understood. It seeks to redefine both the offensive and defensive policies of a nation-state. Yet, notwithstanding the above virtue of espionage, its moral aspects, especially concerning the individual privacy of people and the threat posed by intelligence operations, provide a compelling rationale to strike a just equilibrium of national interests with ethical considerations.

Research Question

In what ways has the development of spying practices over time shaped the contemporary security strategies of nations and, on the other hand, how does the lack of universal legal standard regulating espionage affect the international system of states and its intricacies?

Research Objective

This study proposes how the historical evolution of espionage can contextualize a particular appropriation of the concept for contemporary national security policies. This study also demonstrates that espionage is now an integral part of state politics and affects security policies at both the domestic and external levels. The study also includes a discussion about the challenges presented by the absence of international legal instruments on espionage concerning security relations between states and global security issues relations.

LITERATURE REVIEW

Espionage as a Tool for National Security

A large number of studies have been conducted on the importance of espionage historically and how it has affected the political and democratic arenas of states. In this literature review of my study, I will focus on the most important intelligence and security academic works that support my discussion. Espionage is a crucial tool for ensuring national security, allowing states to proactively address potential threats. As discussed

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

by Godefrey (2022) in *Shape or Deter? Managing cyber-espionage threats to national security interests*, one essential instrument of statecraft is espionage. The modern period of nation governments has regulated and institutionalized the profession, which has existed since the creation of organized civilizations, and charged it with industrial-scale secret stealing. Cyber espionage is a logical development for intelligence services that need to steal secrets as societies shift to digital data storage in networked environments. Spies must engage in cyber espionage for intelligence services to provide the intelligence that their countries require (Godefrey, 2022).

Baker (2004) discusses in *Tolerance of International Espionage: A Functional Approach* that even though all developed countries, as well as many less developed ones, engage in eavesdropping and spying against their neighbors, espionage is oddly little defined under international law. Baker (2004) adds that states spy on one another based on their relative power positions to accomplish self-interested aims, according to the realist perspective on international affairs. However, this theoretical approach not only falls short in explaining international tolerance for espionage, but it also fails to effectively convey the cooperative benefits that espionage provides to all international governments.

According to the functional approach to international relations, Baker (2004) argues that governments would cooperate to promote peaceful cohabitation. In essence, proponents of this viewpoint contend that promoting international collaboration through specific, useful activities is the first step toward world peace and democracy. According to functionalists, peaceful relations can be enhanced through international diplomatic cooperation in state security operations as part of national security policy (Baker, 2004). In my opinion, the functional model of international relations offers a realistic way for the states to enhance relations by leveraging spying and intelligence sharing as an integral aspect of national security. Historically, it can be noted that espionage has come of age, where it is no longer only used to get information, but rather as a tool, which fosters not only security but also diplomacy. As Baker (2004) contends, states can minimize the costs of conflicts by pursuing shared intelligence to build up confidence and trust in each other's capabilities and actions, thereby establishing the needed conditions for international stability.

Lartey (2024) supports this idea of integrating diplomacy with state security operations to enhance national security policy. In his article *The Impact of Spying on Diplomacy: Link to Cyber and National Security, and Recommendations,* Lartey certifies that since the inception of statecraft, espionage has been an integral aspect of diplomacy. Ancient civilizations, such as the Greeks and Romans, often engaged in spying on one another. The impact of eavesdropping on diplomatic efforts is frequently a topic of discussion. While many non-state entities are involved in cyber-spying, not all of them are covered by escalation-reducing measures, such as the "red phone" links that exist between major countries. Therefore, starting with a default assumption of innocence appears to be a weak position once it has been determined that such espionage is prohibited (Lartey, 2024).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

Lartey (2014) continues by adding that nearly every foreign actor and the majority of historical people have either spied on or been spied on throughout history. The first recorded spies in the Old Testament are about 3,000 years old, making them the earliest examples of spying, according to Lartey. From other important views, Macrakis (2023) highlights that accounts of spying and intelligence activities throughout Western history provide a wealth of information about the conflicts and interdependencies between politics, war, diplomacy, and intelligence during the Cold War, world wars, and revolutions. As technology and methods have advanced over time, so too have the tools used in espionage. The tools, powers, and vulnerabilities of espionage have been moved to the internet with the introduction of digital technology. However, the fundamental ideas—to obtain valuable or strategically significant information—remain unchanged. (Macrakis, 2023 as cited in Lartey, 2014). In my perspective, the chronology of espionage beginning from the earliest records in the Bible and carrying to this very digital century today proves that there are global politics where espionage is always a game changer. Each new technique of spying employed by a state demonstrates the changing nature of the relations between states, as the states evolve through technology but essentially spy for information still. This adaptiveness is important going by the fact that digital spying is highly embraced in the modern world. Therefore, an appreciation of history could play a significant role in shaping the positive change that could occur within the intelligence networks in the various nations and even among the members in protecting the territorial integrity of their countries.

One of the most covert human endeavors is espionage. It is also one of the most fascinating, as the popularity of spy stories indicates. Macrakis (2023) in his book, *Espionage: A Concise History* reveals the true nature of espionage and lifts the curtain on the field. Macrakis (2023) guides readers through the murky realm of espionage in a surprisingly straightforward and succinct way, covering everything from the terminology and methods of spy craft to its function in global politics, its bureaucratic foundations, and its evolution in the face of contemporary technology. With the extra layer of secrecy and deceit, espionage is a mirror of society and human frailties (Macrakis, 2023).

Building on the realities of espionage activities that Latrey (2014) and Macrakis (2023), the international nature of espionage poses a significant challenge, but there are several ways to mitigate its effects. When countries are reluctant to use military force to achieve their objectives, diplomacy becomes an essential unifying factor. As long as the importance of international secrets remains, both bilateral and multilateral diplomacy will be critical. Engaging in cooperative dialogue about shared rights, principles, and military standards can help isolate aggressive governments and promote more favorable practices. The situation between Russia and the UK illustrates how diplomacy can help limit risky actions, particularly in the context of the Ukraine issue. Furthermore, while NATO's cyber defense and UN programs prioritize national security in non-legal conversations regarding cyber arms limitation, the UK can decide on suitable countermeasures by classifying espionage as a national security concern. There is no reason why ambassadors cannot denounce hostile states that engage in espionage, particularly when such operations constitute a threat to national identity and reveal

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

undercover agents. Diplomatic techniques can also conflict with national security concerns (Latrey, 2014; Macrakis, 2023).

According to these views of Latrey and Macrakis, I see that the current global system of espionage shapes severe security crises and difficult problems due to its lack of ethical principles that scheme the approaches that should be followed to protect the national interests of people; however, diplomacy can mitigate these repercussions by incentivizing communication among allies and empowering the measures of countering espionage, in addition to isolating aggressive nations. States that are involved in direct espionage must be condemned by diplomats, especially as they put the national interests of other countries at stake. Espionage is indispensable to securitizing states and reinforcing the national capabilities to fight back external espionage threats.

The Ethical Dilemma of Espionage

As espionage is legalized and justified to securitize and safeguard national interests, it also arouses crucial and sensitive moral issues regarding the operatives of espionage, the secret agents. In Huband's (2013) *Trading Secrets*, the moral inferences of carrying out intelligence operations are apparent throughout the narrative of the book, especially in cases where personal freedoms are invaded in the name of national security. The narrative presents several examples of how the CIA conducted intelligence procedures and the controversial considerations they adopted to accomplish intelligence missions in countries such as Sudan and Afghanistan. *Trading Secrets* book for Huband (2013) holds facts of how humanitarian law was breached by interrogators and the indiscriminate policy they adopted when investigating the suspects in prisons, Guantanamo is a clear example of torture and oppression the innocents faced despite their unawareness of the indictments. Punishing the criminals who were involved in the 9/11 attacks was supported by the international community and rectification by the United Nations. The American president George W. Bush during that time launched the war against terrorism to suppress terrorism in the world (Huband, 2013).

Huband (2013) states and proves in his book *Trading Secrets: Spies and Intelligence in an Age of Terror* the trouble with counter-intelligence procedures:

The trouble with counter-terrorism intelligence is that it is coming from all sorts of different areas. It is a question of: what is useful? There are market forces operating-people try to sell it to you, and discrimination between good intelligence and rubbish is very difficult. You are in a balancing act the whole time. (Huband, 2013, p. 142).

M (2023) explores the profound moral issues of intelligence and espionage in *Unveiling the Shadows: The Ethical Dilemmas of Espionage*, stressing how the lines separating good and wrong are frequently blurred. M (2023) explores the difficult moral dilemmas raised by decisions like choosing to "disappear" people for national security reasons and asks when they could be appropriate. M (2023) also addresses the moral dilemmas raised by developments in surveillance and cryptography, balancing the necessity for security with the right to privacy.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

M (2023) argues that the secret agencies strike a very careful balance between national interests and adherence to international law and human rights, his article also discusses the ramifications of geopolitical conflicts, such as China's ascent and Iran's nuclear aspirations. According to the analysis of *Unveiling the Shadows: The Ethical Dilemmas of Espionage*, I see that espionage literature readers are to examine the moral conundrums present in this linked and frequently murky field and advocate for a fuller understanding of the complexity of espionage and as Huband emphasizes that “the only way of understanding what is going on is by having someone inside (Huband, 2013, p. 142).

DISCUSSION

Technological Espionage in the Modern Era: International Law and Intelligence Collection

As depicted in Huband's book *Trading Secrets* (2013), spying is no longer practiced in the same way as it used to be. It has changed with the increase in technology and realignment of political power in the current world. The contention is that in modern times, espionage is not only further reaching and advanced but the activities it incorporates modern-day technology and cyberspace. There are also issues of global consensus on the laws of espionage where each country has its laws and policies that promote national security and relations between states. As a result, espionage has evolved from a simple secret activity that serves only military objectives to a diversified instrument that serves in national security and geopolitical strategies. In particular, cyber espionage has arisen as a serious national security danger. The hazards accompanying cyber-espionage are significant and variate from state-sponsored hacking to the theft of confidential government data (Huband, 2013). Although *Trading Secrets* was composed before the big revolution and sophistication of cyber war technology, its topics and introduced issues and theories regarding espionage have been effective up to now, such as cyberwarfare, signifying the immortal fact of either espionage's positive or negative influences on national security.

For centuries now, espionage as a socially accepted vice has been prevalent in the polity and military strategy of different societies, facilitating its development into the intelligence operations we see today. According to Richmond’s (1998) book *Spies in Ancient Greece*, the Bible (Joshua 2:1) ancient Greece, and ancient China all refer to spies. With more than a hundred international intelligence services currently in charge of similar operations and operating in nations with varying levels of economic development, espionage has persisted and developed. However, there is no international regulation of espionage in peacetime, despite it being such a common technique (Richmond, 1998). Military theorists see like Reynolds (2004) on BBC News in his discussion of *the world’s Second Oldest Profession* that espionage has been around for a while. Indeed, it is frequently called the “second oldest profession in the world” (Reynolds, 2004). In my view, the references to the history of spying in books like Richmond (1998) and the recognition of the continuity of such a practice over time accentuates the complications of the issue.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

One of the major ethical concerns posed is that there are no worldwide bylaws restricting the use of espionage even in times of peace. Moreover, to borrow a phrase from Reynolds (2004), it is easy to understand why this practice is referred to as being the “second oldest profession” – and this suggests that given its nature and the scope of international relations, it is a central issue that must be addressed in terms of ensuring accountability and laying down the regulatory framework.

The available historical accounts erect a significant but understated image of the importance of espionage in uncovering threats faced by the country from its internal enemies, emphasizing the shortfall in the studies/analyses of covert intelligence operations on the other. Richmond (1998) argues that secret spies who attempted to uncover internal dissension and conspiracy will only be mentioned in passing. According to Richmond, all Greek states were perpetually at war, whether declared or not. Even in the present era, no two sovereign states have the same interests. In both peacetime and conflict, governments will try to find a way to protect their secrets while identifying those of the other side. Very little about Greek spying during peacetime is known to us. Richmond (1998) highlights that the Greek States had the option to use war to achieve their goals when diplomacy failed. A strategic plan of intended operations is necessary for war. In the current environment, the plan must be developed with the assistance of numerous experts and must be planned well in advance, according to Richmond. I think this historical view is important for appreciating the modern intelligence operations of states where states find themselves trying to achieve a balance between secrecy and transparency. The need for operational art in intelligence gathering has no expiration date. It speaks to the dilemmas one faces with relations between nations. In the age of globalization, as past practices show, there is still a present need for spying as a means of politics due to international competition.

The staggering growth of data accessibility in the cyberspace arena has enhanced the worth of acquiring target intelligence with an offensive approach, and at the same time, the need for effective measures of cyber defense. According to the New York Times (2016, Oct 21), because of the vast amount of data that is now available, cyberspace simultaneously increases the value of acquiring offensive information and the need for cyber defensive measures. Cyber intrusions, which target a wide variety of targets, have become a common threat. Motivated by this structural development, my study argues that governments must define more precise rules for what constitutes acceptable espionage. They can accomplish this by defining specific espionage actions that circumvent key state concerns. Therefore, using cyber technology to accomplish the objectives of traditional espionage is known as cyber espionage. I contend that with the ever-increasing amount of digital data, states should modify their concept/law of what is acceptable espionage practice. Given the growing levels of cyber espionage, there is a need for National Security considerations, with the safeguarding of ethical standards as one of the priorities. Such a provision can help remove the excesses of cyber ingression, especially in protecting a nation’s interests in this global landscape.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

The ambiguity surrounding the legal framework of espionage extends to international law as well, as emphasized by Forcese (2011). Forcese (2011) explains in *Spies without Borders: International Law and Intelligence Collection* that the definition of espionage in international law is unclear. It should be noted that while international law is ambiguous over whether states generally have the legal authority to spy on other states, it is more obvious that specific espionage-related activities are prohibited. For instance, the use of torture and cruel, inhuman, or degrading treatment to obtain information is expressly forbidden by international law.

The varied geography of espionage is highlighted by Forcese (2011), who explains that intelligence collection can take place in domestic, international, and transnational contexts using both electronic surveillance and human sources. Forcese provides examples of how human intelligence might entail secret communication between an agent and a source, which could occur across national boundaries or within the same nation, like an embassy staffer in a foreign capital. Similar to this, electronic surveillance might start locally, traverse international borders, or even be transnational, with one state keeping an eye on communications from facilities in another. The geographical terrain of intelligence operations is complicated by these many types of espionage (Forcese, 2011).

Regarding Human Rights Restrictions on Spying, Forcese (2011) appears to concur with Huband's (2013) scathing critique of CIA interrogation practices in *Trading Secrets*. International human rights standards may be applied in response to both electronic surveillance and human intelligence. As previously said, gathering information from human resources, or human intelligence, may entail questioning, which raises concerns regarding how these interviews are conducted. For its part, electronic surveillance may—in fact, frequently do—involve covertly monitoring behavior or communications, raising concerns about privacy and individual rights (Forcese, 2011; Huband, 2013).

According to Baker (2004), the use of espionage by states is common, and there is no international agreement that forbids the practice. Baker (2004) in *Tolerance of International Espionage: A Functional Approach*, Baker ensures that states' widespread use of espionage and the lack of clear international legislation make the practice acceptable. A conventional standard for the permissibility of peacetime espionage has been established due to the absence of an explicit historical restriction in international law (Baker, 2004). I am in accord with the criticisms forwarded by Forcese (2011) and Huband (2013) on the concern of ethics within the practice of espionage practices concerning human rights.

Espionage, as Baker (2004) observes, is problematic since there is no concrete international legal framework governing it. This is especially so since its non-regulation can lead to abuses that offend individual rights. Human rights principles should form an integral part of the intelligence-related operations of a state, lest the need for security overrides the protection of an individual’s privacy and dignity. It is with these challenges in mind that strong and comprehensive ethical codes of conduct have to be developed.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

Governments, aid agencies, and businesses have recently become increasingly critical and opposed more and more espionage operations (Deeks, 2015). While there isn't a comprehensive international legal framework governing surveillance activity, Deeks (2015) argues in *An International Legal Framework for Surveillance*, that existing international regulations provide some guidance. These regulations suggest that when states engage in surveillance, they should consider individuals' private rights and the sovereignty of other nations.

However, with the rapid advancement of technology, a more robust legal framework is necessary to ensure that surveillance practices comply with global standards. Despite this growing opposition, there has not been a widespread movement to dissolve intelligence agencies. Various sources, including states and organizations, have voiced their concerns. Notable measures, such as the U.S.-China treaty on economic espionage and the expulsion of Russian spies, illustrate the responses to criticism regarding surveillance and intelligence efforts. These reactions have been influenced by significant events, including the Snowden revelations and Russian interference in U.S. elections. Although there may be future calls for intelligence organizations to align their operations with societal values and regulations, espionage remains generally accepted under customary international law (Deeks, 2015).

Deeks (2015) argues that Edward Snowden's disclosures revealed the extensive electronic monitoring conducted by the US National Security Agency and its international partners. These revelations showed that surveillance targets both private individuals and foreign leaders, raising awareness of the widespread nature of global foreign surveillance. Despite concerns expressed by foreign nationals, scholars, and state leaders, international law has largely remained silent on the issue of foreign surveillance. Historically, no government, court, or treaty has applied international legal norms—such as the privacy protections found in human rights treaties—to the intelligence gathering from foreign nationals. However, this trend is beginning to change. Various UN agencies, courts, businesses, and individuals affected by foreign monitoring are now advocating for stricter legal regulations (Deeks, 2015).

Deeks enlarges the view when highlighting that the world is currently at a crossroads, as governments gain increased ability to intercept electronic communications, which often contain both sensitive and irrelevant data. These developments are occurring alongside the rapid evolution of electronic communication across borders. Governments defend surveillance by asserting it is essential to address dangers posed by non-state entities, including terrorism and the spread of weapons of mass destruction (WMDs).

This intricate scenario presents the difficulty of reconciling individual privacy with security requirements. Deeks (2015) argues that addressing this dilemma requires the application of international law. Establishing procedural standards for foreign surveillance, in response to regulatory demands and the evolving human rights landscape, could help find a compromise between security and privacy, according to Deeks.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

Building on the discussion above, I believe that developing cyber capabilities is essential for protecting the technological assets and privacy of states. In a similar vein, Waxman (2006), in his article *Cyber-attacks and the Use of Force: Back to the Future of Article*, argues that if the cost of developing cyber capabilities is lower than that of traditional espionage techniques, nations with limited traditional espionage resources may choose to enhance their cyber espionage activities to gain more influence on the international stage. However, countries with strong existing cyber espionage programs are likely to resist any efforts that threaten their dominance. These nations would not benefit from an anti-cyber espionage treaty, while weaker states may view restrictions on the development of cyber espionage as oppressive, particularly as they try to close the intelligence-gathering gap (Waxman, 2006).

The interplay between strategy and law can be analyzed as a relationship that mutually influences the two entities within it. In his article, Waxman (2006) makes two main claims. First, he argues that strategy plays a significant role in the evolution of law, emphasizing the dynamic relationship between the two. Waxman highlights the reciprocal nature of this influence: strategy impacts law, and law, in turn, shapes strategy. While many discussions about cyberattacks focus on how international law should adapt to new technologies, Waxman (2006) points out that establishing clear legal interpretations is challenging. This is due to the ongoing interactions involving various stakeholders, each with different interests and capabilities, resulting in a series of moves and countermoves.

Waxman addresses the challenges of achieving a global agreement on legal frameworks for cyberattacks. To effectively address cyber threats, the United States has aimed to update its understanding of international law, especially the U.N. Charter. Nevertheless, the complexity of cyber activities and the varied geopolitical objectives of major stakeholders make it challenging to create a consistent international legal framework. Waxman suggests that American officials should be prepared to navigate a contentious and unpredictable legal landscape as a result.

While multilateral efforts to regulate cyberattacks should continue, it is important to acknowledge their inherent limitations within the broader context of security strategy (Waxman, 2006). I agree with Waxman’s point about the challenges of building an integrated international legal system for activities in cyberspace. Because of the fast pace of technological advancements and the conflicting ambitions of countries, it is hard to put in place global rules. In this regard, while it is important to focus on negotiations and discussions that involve many parties, it is also important to understand the constraints of national security and the dynamic complexities of the cyber environment. It is important for states, particularly the USA, to be proactive and flexible in their legal and diplomatic approaches due to the emerging problematic issues.

All in all, it can be said that the interplay between strategy and the law and international relations can be seen in the changing landscape of intelligence which comprises both traditional and non-traditional forms of intelligence, including cyberspace. Electronic surveillance has become more and more common oftentimes exceeding geographical and individual boundaries as proved by the experiences of Edward Snowden.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

These disclosures have raised legal challenges and calls for greater control. Also, the situation becomes even more perplexing with the introduction of ‘cyber’ spying, where the great powers do not want to embrace any such limitations that can potentially compromise their advantages over others, while the rest of the countries are eager to grow their attacks to invest in this domain. Spying practices have transformed over the centuries, with present-day methods including high-tech spying. The most recent example is Edward Snowden's case in 2013, which revealed the prevailing tensions between national security and personal privacy concerns, while also offering the recent claims of Chinese cyberspace espionage in the COVID-19 vaccine development. As we keep on exploring the chronology of the art of spying, it stands evident that the international community must devise better mechanisms to curb the new threats that are already apparent.

International law is finding it increasingly difficult to cope with challenges such as cyber warfare and espionage focused on foreign nationals within their own territories with the law technologies tends to be ahead of the definitions. Such a scenario results in a situation where fresh forms of spying and invading privacy may succeed in the environment created since the law may not provide sufficient protection. Nye and Deeks have noted and elaborated on the challenge of consolidating all these actions into a global agreement because the stakeholders’ interests are often in conflict, and their strategies are often not the same. However, even so, the scenarios in which laws are amenable to change owing to new emerging risks point to the fact that there is a need to strike an equilibrium between the degree of sovereignty that can be exercised by a state, privacy of individuals and the security needs in the world that is increasingly becoming interlinked. The relationship between strategy and politics is dynamic, and there is a tendency for the states to look for an acceptable compromise in response to the political legal environment which is ever-changing and turbulent. This is how the scope of intelligence activities is going to be defined and constrained in the years to come.

METHODOLOGY

The Research Methodology involves a combination of historical analysis, review of existing literature, and application of theoretical concepts from intelligence studies.

1. Literature Review: This section examines historical sources and scholarly works on the subject of spying spanning from different eras up to the present. Attention is given to such works that present spying in different regimes – the tactics used, the tools, the ethics, and the order in which the practices and technologies became available.
2. Historical Analysis: The study draws upon the history of previous intelligence systems, especially those meant for overthrowing governments in a terrorist fashion, to explain the evolution of espionage as well as its effects on national security. For example, I used those cases where coding practices changed as a result of particular events in history or how intelligence agencies were created and developed by the state.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

3. Theoretical Framework: It is appropriate to state that this study operates within the parameters of political science and security studies' definitions of intelligence and national security. Such theories helped in analyzing the use of espionage as a weapon of national security, especially as it concerns combating terrorism. Issues such as balancing civil rights with the need for monitoring, the moral implications of covert activities, and the purposes fulfilled by intelligence were examined.
4. Comparative Analysis: I looked at the practice of espionage in various historical periods and cultural contexts to trace the trends, similarities, and differences. This sheds light on the evolution of espionage based on external factors like technological progress and shifts in power dynamics.

FINDINGS

Espionage's Continued Significance in National Security

Espionage in all forms remains a critical component of any state’s national security apparatus despite a growing wave of opposition against some methods of spying as in the recent actions of Edward Snowden or the outrage concerning Russian meddling in elections. Today’s standards of international law still, however, view espionage as a normal activity. However, most countries are under pressure to adopt monitoring mechanisms that are commensurate with evolving societal expectations, meaning that there is a growing tendency towards more ethical intelligence practices.

The Transition to Cyber-Espionage

Over the recent years, states with weak traditional counter-intelligence resources have increasingly been leaning towards cyber counter-intelligence as a less expensive means of engaging in global competition. According to Waxman (2006), many governments use it tactically to enhance their repositioning against more powerful states. In comparison, states possessing advanced means of cyber espionage do not accept any terms or containment structures that would curtail their activities, preferring to retain the upper hand. This technology change suggests changes in the practice of espionage, as well as its inclusion as part of present-day security policy.

Establishing International Legal Frameworks Presents Difficulties

The growing challenges of cyber espionage and foreign surveillance are the issues that Deeks (2015), as well as Waxman (2006), have mentioned surpassing the extended borders of international law. Edward Snowden’s leaks, on the other hand, revealed how hard it was to control the state-powered snooping conduits if also high human rights and privacy concerns were to be observed. Also, due to the diverging strategic aims of the powerful countries boycott the establishment of such a legal order. This situation in turn renders practitioners working in this domain “to exist above the law”, as hacking activities and the means to conduct such operations are largely unexplained and, in most cases, unregulated.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

Strategic Interaction Between Espionage and the Law

Strategy and law are interdependent and cannot be referred to as distinct cases. This is because the strategic operations of States, either clandestinely or through counter operations, compel a rethinking of legal parameters, which in turn shapes later strategic parameters. This system of checks along with risks implies that there will ever be many legal bounds, an aspect of espionage practice that will expand.

Security and Privacy in Balance

The rapid growth of electronic communications, together with the ever-increasing power of governments to surveil, poses a significant problem when trying to achieve an equilibrium between security and privacy. The authorities argue that control is necessary to reduce the threats posed by terrorists and the proliferation of arms. Conversely, civil activists and international organizations request stronger regulation of privacy. In this regard, Deeks (2015) brought attention to the issue, noting the challenges faced in controlling foreign intelligence activities in a way that would balance the demands of national security and the right to privacy of individuals.

CONCLUSION

The current dialogue regarding the morality and legality of espionage is becoming more intriguing. With countries depending on cyber espionage to gain an upper hand, there is an urgent appeal for international law to develop mechanisms of control against risks and technologies that emerge. The interplay between privacy, security, and the sovereignty of a state will to a great extent, define the existing laws and strategies regarding incorporation of espionage in national security operations. The development of the concept of espionage over the years has been illustrative of the salient nature of intelligence gathering in both state security and inter-state politics which calls for better management policies and ethical frameworks as far as intelligence activities are concerned.

References

1) Andrew, C. (2012). *The defence of the realm: The Authorized History of MI5*. Penguin UK.

2) Andrew, C. (2018). *The Secret World: A History of Intelligence*. Penguin UK.

3) Baker, C. D. (2004). Tolerance of international espionage: A functional approach. *American University International Law Review, 19*(5), 1091–1143.

4) Childers, E. (2011). *The riddle of the sands* (Dover Thrift Editions). Dover Publications.

5) Deeks, A. (2015). An international legal framework for surveillance. *Virginia Journal of International Law, 55*(2), 291-328.

6) Farney, J., & Kordan, B. S. (2005). The Predicament of Belonging: The Status of Enemy Aliens in Canada, 1914. *Journal of Canadian Studies*, *39*(1), 74–89. https://doi.org/10.1353/jcs.2006.0003

7) Forcese, C. (2011). Spies without borders: International law and intelligence collection. *Journal of National Security Law & Policy, 5*(1), 179–193.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 11:2024
DOI: 10.5281/zenodo.14213978

8) Godefrey, L. (2022). Shape or deter? Managing cyber-espionage threats to national security interests. *Studies in Intelligence*, 66(1), Extracts.

9) McIndoe, A. R. (2015). *A Pluralistic Imperialism?: Britain's Understanding of Sovereignty at the Signing of the Treaty of Waitangi*.

10) Huband, M. (2013). *Trading secrets: Spies and Intelligence in an Age of Terror*.

11) Jeffery, K. (2010a). *MI6: The History of the Secret Intelligence Service 1909-1949*. A&C Black.

12) *Joshua 2:1-24 – The Spies and Rahab - Enter the Bible*. (2023, November 3). Enter the Bible. https://enterthebible.org/passage/joshua-21-24-the-spies-and-rahab

13) Keil, A. (2023). A very British dictatorship: The Defence of the Realm Act in Britain, 1914-1920. *First World War Studies*, *14*(1), 51–70. https://doi.org/10.1080/19475020.2024.2307040

14) Lartey, S. (2024). The impact of spying on diplomacy: Link to cyber and national security, and recommendations.

15) M, G. (2023, October 15). *Unveiling the Shadows: The Ethical Dilemmas of Espionage*. https://www.linkedin.com/pulse/unveiling-shadows-ethical-dilemmas-espionage-gabriel-mahia/

16) Macrakis, K. (2023). *Espionage: A concise history*. [HTML].

17) Neligan, D. (1999). *The Spy in the Castle*. Irish Books & Media.

18) New York Times. (2016, October 21). *Hackers used new weapons to disrupt major websites across U.S.* http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?rref=collection%2Ftimestopic%2FCyberwarfare&_r=0

19) Reynolds, P. (2004, February 26). *The world's second oldest profession*. BBC News. https://perma.cc/B9KM-E5E5

20) Richmond, C. (1998). *Spies in ancient Greece*. Greece & Rome, 45(1), 1-14.

21) The Quran. (n.d.). Surah An-Naml (27:20-24)

22) Waxman, M. C. (2006). *Cyber-attacks and the use of force: Back to the future of Article 2(4)*. Yale Law Journal, 115(4), 424–425.