A CRITICAL ANALYSIS OF THE LAW OF SPIES AND ITS CONTEMPORARY ISSUES

Khushi Dwivedi[1] & Ms. Apeksha Pandey[2]

[1] BBA LL.B. (H.) X semester, Amity Law School, Amity University Madhya Pradesh

[2]Assistant Professor, Amity Law School, Amity University Madhya Pradesh

ABSTRACT

By historical as well as current perspectives, this study essay analyses the legal systems regulating espionage—often known as the "law of spies"— an ongoing aspect of international relations, espionage crosses the fine line between national security concerns and international legal duties. Although spying is universally done by countries, it exists mostly in a legal grey area without a thorough international legal framework. Especially under the Geneva Conventions, the Hague Regulations, and customary international law, this study examines the conflict between accepted state practice and the restricted legal acknowledgment of spying in international law.

Starting with the historical development of the law of espionage, the study looks at traditional legal tools and customary practices that have affected state conduct. It then launches a thorough analysis of current problems, including cyber espionage, whistle-blower safeguards, state-sponsored surveillance, and the function of non-state players. The legal status and treatment of captured spies, the changing limits of sovereignty in the digital age, and the ethical ramifications of covert operations are all emphasized.

Contemporary problems are investigated using case studies include the Edward Snowden leaks, the assassination of foreign agents, and state-sponsored cyber operations against vital infrastructure. The study further assesses the conflict between the national security demands and human rights, especially the rights to privacy and fair trial. By means of comparative legal research, the paper explores how several countries—including Russia, China, members of the European Union, and the United States—interpret and enforce laws pertaining to espionage.

The paper finally makes the case for the growth of a more consistent international legal system that takes into account both old and contemporary methods of spying. It suggests legal changes designed to guarantee accountability, transparency, and the respect of basic rights without compromising legitimate national security concerns. This study adds to the increasing debate on how an ever more linked globe should reconcile the clandestine character of espionage with the rules of international law.

Keywords: *Geneva Conventions, Hague Regulations, Customary International Law, State Practice, Whistle-blower Safeguards, Cyber Espionage, Human Rights, National Security Concerns.*

1) INTRODUCTION

Covering the body of legal laws and procedures, domestic as well as international, guiding the carrying out of spying and the treatment of individuals involved in espionage is the "law of spies." Though practically all nations practice spying, its part in international law is unclear: it is very used but little governed. Apart from issues of national security, the intrinsic secrecy of intelligence operations has helped to create a fragmented, doubtful, and in many cases politically charged legal system.

Espionage has been handled usually only somewhat addressed within the broad framework of international humanitarian law and the law of armed conflict. Among the first international treaties to specifically name a spy and specify legal consequences of espionage in wartime, the 1907 Hague Regulations Under the Hague

Regulations, Article 29 declares a spy as someone who—stealth or under false pretences in an operational region—intends to provide information to an adversary. Under this structure, captured spies are not eligible for prisoner-of-war status and may be penalised by the holding country following a just trial.

Also recognizing the legal difference between spies and genuine soldiers are the 1949 Geneva Conventions, the foundation of current international humanitarian law. Although the Geneva Conventions provide limited rights to spies, they offer complete safeguards for combatants and non-combatants during armed conflict; hence mirror the conventional view that espionage is an illicit war act.

National rules, which vary greatly across nations, mostly control the legal management of espionage in peacetime. Often citing it as a threat to national security, most countries forbid spying under their local legal systems. Domestic espionage laws usually focus on actions like the unapproved collection or transfer of secret information, the penetration of sensitive institutions, and cooperation with foreign intelligence services. These unclear regulations can be applied to suppress dissent, target whistle-blowers, or silence political opposition under the cover of preserving state secrets.

Especially via cyber espionage, the creation of fresh methods of intelligence gathering has brought the shortcomings of current legal systems to light. Technological breakthroughs have allowed governments and non-state actors to conduct remote espionage, sometimes without physically crossing boundaries or participating in conventional penetration actions. This development has caused intelligence collection and aggressive actions to merge thus creating fundamental challenges for existing legal frameworks in digital environments.

Edward Snowden alongside Julian Assange alongside Chelsea Manning have created a worldwide dialogue about the required transparency levels between national security operations and public welfare. Through specific cases we see the essential nature of transparency which helps separate harmful espionage activities from necessary public disclosures of governmental misconduct.

Legal uncertainty, practical inconsistency, and a growing tension between traditional legal ideas and contemporary intelligence methods define the role of spies. Re-evaluation and improvement of the legal requirements directing this secret but essential field of international relations gets even more important as countries develop and sharpen their intelligence capabilities.

2) LEGAL AND THEORETICAL FOUNDATIONS OF ESPIONAGE

2.1. Forms and Definition of Espionage

Generally speaking, espionage is the secret collection, transmission, or usage of information regarded as secret or sensitive—usually concerning to national security, defence, or intelligence—without the permission of the data holder. Mirroring more broad shifts in geo-politics and technology, spying—traditionally connected with state players—now also includes non-state entities, private contractors, and online platforms.

Depending on the means of intelligence gathering, espionage can be divided into several kinds:

- *Human intelligence (HUMINT)* gathers data from human sources. It may involve infiltration, monitoring, informer recruitment, or actual interaction with operatives stationed in international militaries, governments, or other organizations.
- Intercepting electronic signals including phone conversations, internet data, and radio communications is known as *signal intelligence (SIGINT)*. With states spending significantly on surveillance and data collecting capacity, this approach has exploded in the digital era.
- *Cyber Espionage:* Contemporary and growing popular kind of espionage wherein unauthorized access to computer systems, networks, or digital infrastructure is done with the aim of stealing sensitive data. Often state-sponsored and carried out remotely across borders, attribution and enforcement are legally difficult. Often used for strategic or military analyses, *imagery intelligence (IMINT)* and *measurement and signature intelligence (MASINT)* are information obtained by way of sensors, technological approaches, and satellite imagery.

Although espionage's goals stay same—collecting intelligence for strategic benefit—the approaches keep evolving, which has major repercussions for both national and international legal systems.

2.2. Separation of Legal from Illegal Fighters

The general law of armed conflict—especially as stated in The Hague Regulations (1907) and the Geneva Conventions (1949)—strongly affects the legal classification of those engaged in espionage. These tools differentiate spies, unlawful fighters, and lawful fighters.

- *Legal combatants* are members of a state's armed forces or militias who follow the rules of war openly. Should they be taken, they are eligible for prisoner-of-war (POW) status and attendant safeguards.
- *Unlawful Combatants:* People who engage in fighting without legal recognition as such. Among these are spies, mercenaries, and occasionally terrorists. They can be prosecuted for their conduct; they are not entitled to POW protections.
- According to *Article 29 of the Hague Regulations*, a spy is someone who, working secretly or under false pretences, gathers or attempts to gather information in the zone of operations intended for sharing to a hostile party. Even if caught during war, spies are not eligible for POW status and might be tried and punished by the capturing state following a fair trial.

Reflecting the mistrust and stigma espionage carries even in wartime, this legal framework separates sharply the treatment of conventional combatants and those engaged in intelligence operations.

2.3. Treason versus Whistleblowing versus Espionage

Legally separate ideas, espionage, whistleblowing, and treason are sometimes intertwined in public debate:

- For strategic, political, or financial advantage, espionage entails the unlawful gathering and passing of secret information, usually to a foreign entity. The agent's allegiance is to the receiving power, usually a hostile country.
- Usually in the public interest, whistleblowing is the act of revealing illegal activity, corruption, or other unethical behaviour inside of a company. Although it can include the revelation of secret or classified information, the goal is normally to advance accountability and transparency instead of support a foreign country.
- Typically defined in national law, treason is acts that betray one's country. It might involve helping adversaries during times of war, trying to overthrow the government, or activities that endanger national security. Treason is a more general political crime that may or may not include espionage.

The main difference is in the goal and target of the action. Espionage helps a foreign power; whistleblowing usually serves to warn the public or supervising agencies; and treason degrades the sovereignty and constitutional order of a country. Under legislation pertaining to espionage or treason, whistle-blowers have, however, frequently been prosecuted—exposing the legal and moral conflicts surrounding these definitions.

2.4. Customary International Law and State Practice in General

There is no all-encompassing global agreement controlling spying under non-war circumstances. The legal environment is hence greatly influenced by state practice and traditional international law. Although nations worldwide denounce outside spying operations against them, they often participate in comparable activities themselves, hence the general approach is one of pragmatic tolerance.

- State Practice: Under their national legislation, most nations criminalize espionage with severe punishments including life imprisonment or capital punishment. Concurrent with many other states run elaborate foreign intelligence networks, including surveillance operations, cyber penetration, and recruitment of foreign agents.
- International law mostly steers away from controlling peacetime espionage. The UN Charter stresses non-intervention and sovereignty, which espionage may breach, but there is no clear outlaw of spying. Although only to some degree, the Geneva Conventions and Hague Regulations apply during times of conflict.
- Certain traditional standards have emerged regarding the treatment of captured spies, particularly the need of a fair trial. These standards, however, are applied irregularly and usually subordinate to national security considerations.

3) LAW OF SPIES' HISTORICAL EVOLUTION

The origins of spying extends past to prehistoric communities; Sun's military treatise, "The Art of War," classifies spies into various groups and highlights their crucial role in warfare. During the mediaeval period, monarchs and dynasties established espionage among their courts through the use of undercover officers, informants, and messenger connections for inner monitoring and defence reconnaissance missions.

Spying treatment is included in *the 1907 Hague Rules*, which define a spy as someone who gathers information in hostile soil covertly or beneath false pretences with the goal of providing it to the opposing side. These

regulations included provisions such as not qualifying for prisoner-of-war classification, allowing just trials for captured spies, and not considering open intelligence collecting by a fighter.

The *Geneva Conventions of 1949* further advanced international humanitarian law, stating that a spy caught and returns to their own armed forces is not liable for past acts of espionage. However, if apprehended in the act, the person could be stripped of POW safeguards and prosecuted. These treaties represent the first legal treatment of espionage codification under international law, reflecting a consensus that while espionage is an expected aspect of conflict, it goes beyond the limits of protected combatancy.

Espionage became a major and institutionalized form in the 20th century during the *Cold War and World War II.* Secret service agencies conducted clandestine activities during both World Wars, which included treason operations, the exposure of sensitive data and encryption systems, and the distribution of propaganda. Military authorities typically condemned or detained agents apprehended during wartime conflicts.

The legal reaction to espionage differed greatly across countries, with accused spies often used as political pawns in both the East and West, often denied due process. The Cold War further emphasized the gap between state practice and international law, with legal protections for spies remaining little even as spying was prevalent and sometimes state-sanctioned.

The legal position of spies during international armed conflicts depends on foundational guidelines from both the Hague and Geneva treaties. The legal definition of spying applies exclusively to wartime situations where information is collected through deceptive means across hostile territories. The situation becomes unclear due to factors such as individuals collecting intelligence through open means or electronic channels, cyber technicians operating from remote locations violating territorial and physical presence requirements, and non-state actors participating in asymmetric warfare alongside insurgent groups and terrorist organizations. When spies are captured, their treatment varies due to domestic political needs and strategic interests outweighing the standard application of international law.

4) MODERN LEGAL SYSTEMS AND NATIONAL POLICIES

4.1. Domestic Espionage Legislations in Leading Nations

- United States:

The Espionage Act of 1917 makes it illegal to handle, transmit or retain defence information without permission.

Modifications to the law extended its reach to both whistle-blowers and journalists.

The Foreign Intelligence Surveillance Act (FISA) along with selected parts of the Patriot Act serve as other critical statutes.

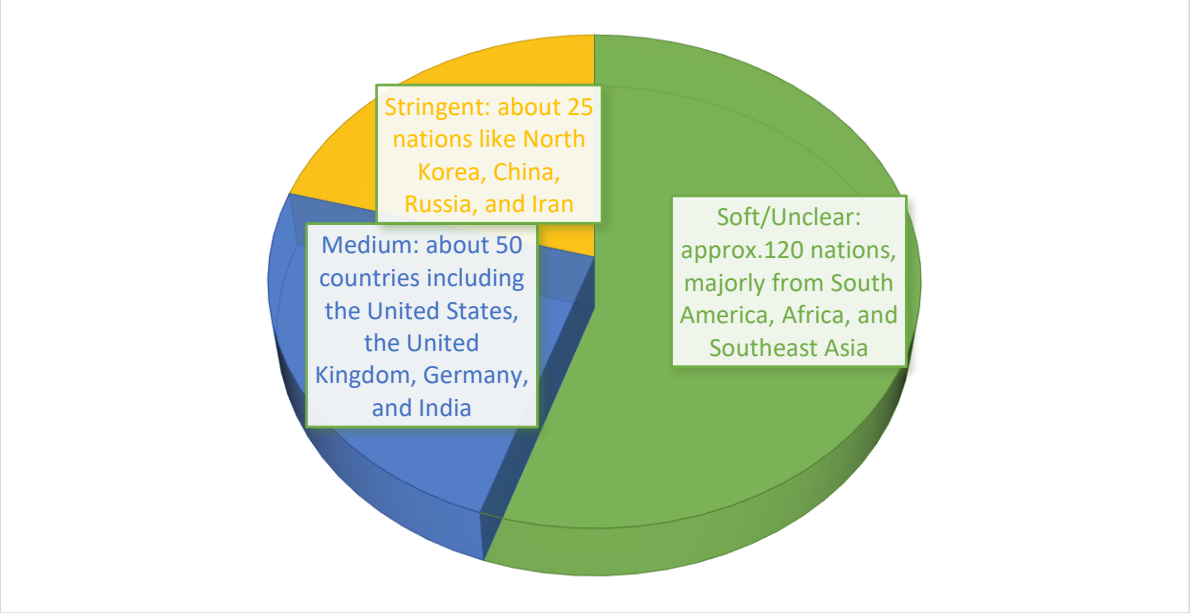

Chart-1: Country to country distribution of the severity of spying laws

- United Kingdom:

The Official Secrets Acts from 1911 and 1989 establish the essential framework for handling espionage matters in the United Kingdom.

The 1989 version of the act restricted access to particular types of official data.

The National Security Law of 2023 updates the laws pertaining to espionage.

- Russia:

Spying is considered a serious unlawful activity and a crime as per Russia's Criminal Law.

The Federal Homeland Security Service has broad powers to conduct enquiries and detain people.

- China:

The Counter-Espionage Law of 2014 with its 2023 modifications and the National Intelligence Law of 2017 require organizations to assist national intelligence operations.

The definition of espionage in China is broad and results in substantial legal consequences.

- European Union:

Germany's Criminal Code and France's Penal Code along with other member state laws are in effect throughout the European Union.

Table-1: Indian Regulatory Framework against Espionage

S. No.	Statute	Aim / Scope	Essential Provisions	Punishment	Comments
1.	1923 Official Secrets Act (OSA)	Forbids disclosure of confidential information in order to prevent unauthorised ownership or dissemination of official knowledge that might jeopardise national security.	• Prohibits espionage, exchange of covert information • Includes defence infrastructure and military installations • It extends to both citizens as well as foreigners	Has a maximum penalty of 14 years in jail.	The legislation is from the period of colonial rule and is unclear about contemporary dangers such as cyber espionage.
2.	Sections 121-124A of the Indian Penal Code (IPC)	Deals with offences contrary to the state.	Section 121 deals with waging war against the country of India, Section 123 with hiding intentions to conduct war, and Section 124A with sedition.	Section 121 carries a death sentence or life in prison, while Section 124A carries a maximum sentence of three years.	Frequently brought up in politically delicate spying accusations.
3.	Act of 1967 on the Prevention of Illicit	To stop illegal and terrorist actions	• Proclaims associations to be illegal.	180 days of custody with no charge or lifetime in jail.	Often employed in prominent cases implicating foreign spies.

	Activities (UAPA)		• Implemented by terrorist organisations to imprison alleged spies • Enables NIA to conduct investigations		
4.	The 1980 National Security Act (NSA)	Detention without charge for national security	• Utilised when spying seems likely but difficult to establish • It permits incarceration for a maximum of 12 months with no trial.	• Not punitive but preventive.	• Allows for swift intervention yet is criticised for avoiding due process.
5.	Section 66F of the Information Technology Act of 2000	Addresses cyberterrorism and internet spying	Theft of data, illicit access, and major infrastructure breaches	For e-terrorism, life in jail	Pertinent to situations concerning hacking or internet spying
6.	The 1985 Act concerning the restrictions on the Rights of Intelligence Organisations	Restricts the privileges granted to intelligence personnel	• Forbids them from speaking to the general population or press. • Limits establishing unions or alliances.	Criminal and disciplinarian penalties	Used to preserve confidentiality with RAW, IB, etc.
7.	The 1885 Telegraph Act and the 2008 IT (Amendment) Act	Communication monitoring and interception	Enables the authorities to observe potential intelligence operations by intercepting mails and phone conversations.	Judicial and administrative monitoring are applicable.	Encourages the collection of surveillance data against informants.

4.2. Right to Procedural Justice and Frameworks of Intelligence Oversight

Prevention of abuse of authority by intelligence services depends on mechanisms of intelligence oversight and due process rights. While the F*oreign Intelligence Surveillance Court* oversees, the *House and Senate Intelligence Committees* offer supervision in the United States. While the European Union countries have different oversight mechanisms, the *Investigatory Powers Tribunal of the UK* and the *Intelligence and Security Committee of Parliament* examine intelligence operations. Oversight is little or symbolic in Russia and China; suspected spies have little or no clarity. Therefore, for suspected spies, due process rights differ greatly across different jurisdictions.

4.3. State Confidentiality Theories and National Security Regulations

- The United States' State Secrets Advantage: This gives governments the ability to keep confidential data from being revealed during court cases.

- UK and EU: Permits tribunals to decide in opposition to governments in monitoring and confidentiality incidents by striking an appropriate equilibrium between national security concerns and the ECHR.
- China and Russia: Both countries have broad and ambiguous state confidentiality legislation that permit detention, information constraints, and disapproval inhibition with little accountability or legal redress.

4.4. Comparative Regulatory Safeguards to Suspects of Espionage

- Fair Trial Guidelines: Liberal democracies provide the right to appeal, the right to legal representation, and the assumption of innocence.
- These safeguards are frequently absent from dictatorial governments, which offer little representation by attorneys as well as concealed court trials.
- Safety measures for Whistle-blowers: Russia and China frequently mistake whistleblowing for treason or espionage; the United States provides modest safeguards that do not apply to media outlets or foreign announcements.

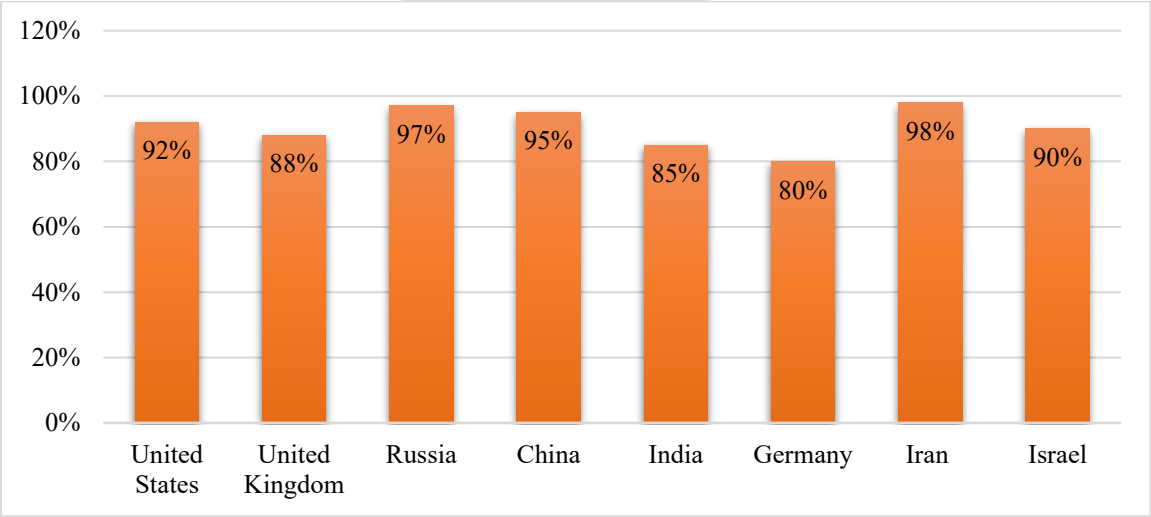

Chart-2: Conviction percentage in major nations' spying cases from 2000 to 2024

5) RECENT DEVELOPMENTS IN THE ESPIONAGE LAW

- The adoption of technological devices to breach networks of computers, database servers, or systems across borders in a way gain sensitive and confidential information is known as *cyber espionage* and *international spying*.
- Legal obstacles include issues with jurisdiction and independence of nation states, confidentiality versus safety, and the absence of globally applicable rules.

Case Examples:

- Stuxnet was employed by the United States and Israel around the year 2010 to disrupt the nuclear initiative of Iran, and Russian government officials were responsible for a significant cybersecurity compromise at SolarWinds during 2020.

Misinformation and Electronic Subversion Promoted by the Government

- A key instrument in contemporary blended warfare and covert operations.

Regulatory and Conventional Lacks

- During peacetime, there are no specific guidelines of what constitutes illegal misleading information.

Identification Issues

- Unidentified substitutes or third-party characters are frequently used in disinformation initiatives.

Free Speech Issues

- The constitutional right to exercise free speech has to be weighed against the attempts of the government to combat misinformation.

The Function of Personal Contractors alongside Non-State Players

- Third-party players such as business organisations, hacktivist teams, and terrorist organisations.

6) THE HUMAN RIGHTS AND MORAL ASPECTS OF ESPIONAGE

6.1. Finding a Balance between Civil Rights and National Security

Civil liberties are frequently restricted on the basis of national security.

- Unrestrained surveillance operations have the potential to undermine democratic principles.
- Particular liberties may be constrained for national security purposes under international law.
- Espionage raises ethical concerns with regard to whether benefits outweigh means because it entails deceit and invasions of privacy.

6.2.) Regulations that control surveillance activities must respect the Fundamental Right to Privacy of individuals.

- A number of legally binding documents, such as the European Convention regarding the protection of Human Rights (ECHR), the International Covenant on the Political and Civil Rights (ICCPR), and the Universal Declaration on Human Rights (UDHR), guarantee a person's fundamental entitlement to privacy.
- Electronic surveillance regulations and other monitoring systems often lead to the violation of this right.

6.3) Fair Trial Guidelines for Lawsuits Associated with Espionage

- Because of highly sensitive data, espionage proceedings frequently depart from accepted legal standards. Exclusive judicial bodies, closed proceedings, and concealed evidence are obstacles to equitable trials.
- The entitlement to a free and open trial by an unbiased, independent and trustworthy court is guaranteed by Article 14 within the ICCPR.
- The rulings of the European Court on Human Rights (ECtHR) highlights that the right to an impartial hearing cannot be completely superseded by national security concerns.

7) LEADING CASE STUDIES

The Legal and Ethical Repercussions of Edward Snowden and the National Security Agency Monitoring[1]

- Snowden's disclosure of confidential files exposing vast worldwide surveillance systems sparked a worldwide discussion about privacy versus mass monitoring.
- The United States Freedom law of the year 2015 limited the acquisition of large amounts of information that impacted decisions regarding the Atlantic region data exchange by the European Court on Justice.

The Julian Assange WikiLeaks scandal:[2]

- Assange, the organization's founder, raised issues related to the freedom of the press and national security after publishing countless classified American documents.
- The United States wants to extradite him back from the United Kingdom on accusations of spying.
- The incident sparked international debates about the significance of non-state entities in intelligence leakage by exposing combat wrongdoings and civil rights abuses.

[1] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York, Metropolitan Books, 2014)
[2] Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy* (London, Guardian Books, 2011)

The Skripal Case:[3]

- In Salisbury, England the Russian Government Relations Unit's agents intoxicated and killed former Russian dual agents Sergei Skripal along with his daughter using a defence-grade neuro substance.
- The incident sparked concerns about intelligence retribution and assassinations that are funded by the state.

SolarWinds Cyber Espionage:[4]

- A highly skilled online attack impaired SolarWinds computer programs, impacting both private companies and government organizations in the United States.
- In addition to highlighting identification and jurisdictional difficulties associated with reacting to technological breaches, the hacking attempt illustrated the unclear legal status of internet spying.

The Stuxnet Mission:[5]

- It was a virus for computers produced by the nation of Israel with the aid of United States to disrupt Iranian atomic centrifuges; the operation wasn't explicitly governed by humanitarian laws around the world.
- Started the modern age of state-funded sabotage and cyberspace warfare.

Huawei Inc. and the Spying Charges:[6]

- The Chinese innovation leader, Huawei Corporation, was charged with business and state sabotage by the United States government, which resulted in barriers to trade, criminal proceedings, and the detention of its Chief Financial Officer Meng Wanzhou in Canadian territory.

7.1. Cases in Indian Espionage

The case of Kulbhushan Jadhav[7]

- Arrest and allegation of espionage and sabotage against a former Indian Navy officer. He was sentenced to capital punishment by the Pakistani military.
- Pakistan violated the Treaty of Vienna regarding Consular Relationships by refusing accessibility to diplomats.
- The International Tribunal for Justice (ICJ), which India presented the matter before, ruled that the Pakistan government had violated the rules of international law.
- The case sparked arguments regarding fair trial requirements and military courts.

The "Black Tiger" Case of Ravindra Kaushik:[8]

- Recruited by RAW, Indian deep-cover operative in Pakistan.
- For years sent confidential information to India before being apprehended and jailed.
- Worked as a non-uniformed fighter, hence breaking the legitimate combatant norm under Geneva Conventions.
- Tortured and perished in Pakistani prison.

Underlined legal hazards and absence of cover for covert operatives in foreign countries.

---

[3] UK Parliament, House of Commons, *Russia: Implications for UK Policy*, Foreign Affairs Committee, Fifth Report of Session 2017–19 (HC 982, 21 May 2018), available at https://publications.p arliament.uk/

[4] CISA, "Cybersecurity Advisory: SolarWinds and Related Supply Chain Compromise," Cybersecurity & Infrastructure Security Agency (2021), available at https://www.cisa.gov/

[5] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York, Crown, 2012).

[6] **United States v. Huawei Technologies Co. Ltd.**, Indictment No. 1:18-CR-457 (E.D.N.Y. filed Jan. 24, 2019), U.S. Department of Justice, available at: https://www.justice.gov/opa/press-release/file/1125021/download.

[7] International Court of Justice, *Case Concerning the Vienna Convention on Consular Relations (India v. Pakistan)*, Judgment of 17 July 2019, available at https://www.icj-cij.org.

[8] Maloy Krishna Dhar, *Open Secrets: India's Intelligence Unveiled* (New Delhi, Manas Publications, 2005) at 147–150.

Sarabjit Singh Case[9]

- Pakistan arrested this Indian farmer who crossed the Indo-Pak border accidently for spying and bomb attacks. He never returned back to India alive.
- Alleged torture, compelled confessions, and lack of fair trial.
- Started national discussions on foreign detainees and prisoner of war treatment.

Pakistani Spy Ring Bust in Rajasthan and Kashmir[10]

- Pakistanis or Indian citizens acting as informants for the ISI who were arrested.
- Charged under the Unlawful Activities Prevention Act (UAPA) as well as under the Official Secrets Act, 1923.
- Raised questions about internal security and foreign espionage influence.

Controversy surrounding Pegasus Spyware[11]

- Investigations turned up possible use of Israeli spyware Pegasus to monitor Indian journalists, activists, opposition leaders, and public figures.
- Claims of violations of right to privacy.
- Appointed an independent expert committee and emphasized constitutional checks on surveillance authority.

8) CRITICAL ANALYSIS AND DEFICIENCIES IN THE PRESENT LEGAL SYSTEM

8.1. Flaws in International Legal Tools

Key global instruments including The Hague Rules and the Geneva Conventions fail to appropriately control or define espionage.

- These tools fail to address technological developments, peacetime espionage, or create important legal ambiguity.
- Organs such the International Criminal Court (ICC) and UN Security Council handle espionage as a political matter, creating a legal vacuum.

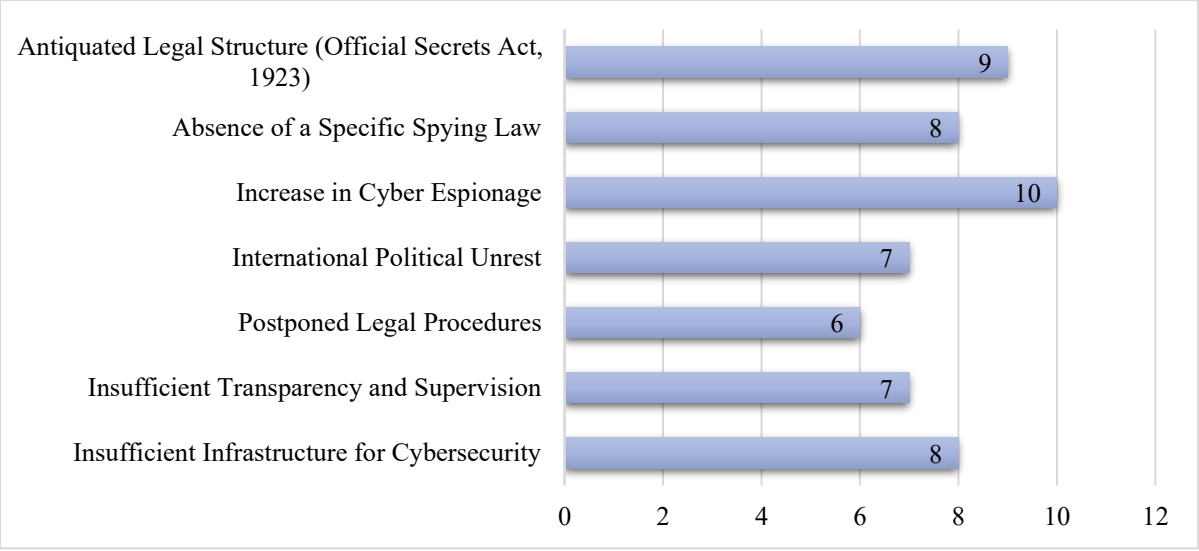

Chart 3: Current loopholes in the Indian Espionage Regulatory Framework

[9] Kuldip Nayar, "Sarabjit Singh's Tragedy Reflects the State of Indo-Pak Ties," *The Tribune*, May 2, 2013.
[10] Press Trust of India, "Pakistan High Commission Staffer Expelled for Espionage," *The Hindu*, 28 October 2016.
[11] Supreme Court of India, *Manohar Lal Sharma v. Union of India*, W.P. (Crl.) No. 314/2021, Order dated 27 October 2021.

8.2. Divergent State Policies and Absence of Consistency

State practice determines espionage law more than agreement does.

- China criminalizes spying under its National Security Law; the U.S. uses the Espionage Act of 1917.
- European nations provide more legal certainty but have varying degrees of enforcement.
- Enforcement and Jurisdictional Difficulties
- Espionage frequently goes across boundaries, therefore raising difficult problems with legal jurisdiction.
- Because espionage is political, treaties like MLATs frequently fail or cannot be used.

8.3. Challenges in Accountability and Transparency

Because of its secret character, espionage usually bypasses public control.

- Whistle-blowers get penal sanctions instead of protection.
- Often held in secret courts, with limited procedural protections and public view, trials of suspected spies lack public awareness.

9) SUGGESTIONS FOR ESPIONAGE REFORM

- Establish a written global framework on espionage separate from whistleblowing, reporting, and cybercrime.
- Categorize espionage types and allocate rules appropriately.
- Establish minimum legal standards for the treatment of captured spies, including fair trial and consular access.
- Understand cyber spying as a unique legal class.
- Define in cyberspace what counts as an attack of aggression or infringement of sovereignty.
- Set up mechanisms for attribution and rules of engagement.
- Coordinate local legislation with global standards on human rights.
- To ensure equal consideration, amend legislations like the Espionage Act (in the United States) and the Statute of Official Secrets (India).
- Give legal backing to whistle-blowers who have worked for the greater good of mankind.
- Improve legal protections, responsibility, and oversight.
- Set up or give autonomous parliamentary committees power to oversee intelligence operations.
- Demand legislative controls for intelligence agencies.
- Protect Privacy Right
- Employ international mechanisms like a UN Special Rapporteur on Espionage and Surveillance.

10) CONCLUSION

Legal bases, historical development, current frameworks, and new issues relating to espionage in both domestic and foreign settings are explored in this study. It exposes the absence of a thorough global legal system that sufficiently covers the whole range of espionage actions. The criminal prosecution of intelligence agents during times of warfare is dealt with briefly by the regulations of the Hague (1907) as well as the Geneva Protocols (1949), however both of these documents are no longer in pertinent to current scenarios and are mostly quiet regarding actors that are not states, non-military espionage, and cyber spying. This legal vacuum has caused reliance on state-centric interpretations, usually influenced by political and strategic rather than constant legal concepts. Comparative study of national legislation across countries including the United States, Russia, China, the United Kingdom, and India has shown marked differences in how espionage is defined, prosecuted, and penalized. Emergent problems including cyber espionage, state-sponsored propaganda, the role of private contractors, and questions of attribution and anonymity are also discussed in the thesis. The ethical and human rights aspects investigated highlight the pressing necessity of harmonizing national security needs with basic civil liberties, especially the right to privacy, freedom of expression, and fair trial requirements. The case studies examined show the real-world effects of legal and institutional gaps, therefore pointing out the risks of unrestrained intelligence operations, the fragility of people caught in geopolitical crossfire, and the limits of present legal remedies.

11) REFERENCES

11.1. Books

[1] Dhar, Maloy Krishna, *Open Secrets: India's Intelligence Unveiled*, Manas Publications, New Delhi (2005).

[2] Chesterman, Simon, *One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty*, Oxford University Press, Oxford (2011).

[3] Luban, David, *Legal Ethics and Human Dignity*, Cambridge University Press, Cambridge (2007).

11.2. Articles & Journals

[1] Schmitt, Michael N., "The Tallinn Manual on the International Law Applicable to Cyber Warfare", *Harvard International Law Journal*, Vol. 54, No. 1 (2013), pp. 247–286.

[2] Ohlin, Jens David, "Cyberwar and the Law of War", *Emory International Law Review*, Vol. 30 (2016), pp. 533–562.

[3] Chesterman, Simon, "The Spy Who Came In From the Cold War: Intelligence and International Law", *Michigan Journal of International Law*, Vol. 27, No. 4 (2006), pp. 1071–1130.

11.3. Government & Official Reports

[1] CISA, "SolarWinds and Related Supply Chain Compromise", U.S. Cybersecurity & Infrastructure Security Agency (2021), available at https://www.cisa.gov/.

[2] UK House of Commons, *Russia: Implications for UK Policy*, Foreign Affairs Committee, Fifth Report of Session 2017–19 (HC 982), 21 May 2018, available at https://publications.parliament.uk/.

[3] Indian Ministry of Home Affairs, *Annual Report 2020–21*, Government of India, available at https://www.mha.gov.in/.

11.4. Websites

[1] International Court of Justice, *Case Law & Judgments*, available at https://www.icj-cij.org/ (last visited May 20, 2025).

[2] Ministry of Home Affairs, Government of India, *Annual Reports and Official Notifications*, available at https://www.mha.gov.in/ (last visited May 22, 2025).

[3] Human Rights Watch, *Reports on Surveillance and Whistleblowers*, available at https://www.hrw.org/ (last visited May 23, 2025).