RESEARCH ARTICLE

AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

THE LEGALITY OF ESPIONAGE IN PEACETIME

Fawaz Najem* and Abdelnaser Aljahani

ABSTRACT

Background: *This research paper examines the legality of espionage during peacetime under the rules of international law. To address this issue, the paper focuses on several relevant international law rules, including the obligation to respect the sovereignty of other states and the prohibition on intervention. Although espionage is a longstanding instrument of statecraft essential for safeguarding national security, it occupies an uncertain legal position. International legal frameworks, including the UN Charter and customary international law, establish obligations such as the respect for state sovereignty and the prohibition of intervention, which espionage activities frequently challenge. The growth of modern surveillance capabilities, especially in the cyber domain, further complicates the legal and ethical boundaries of espionage.*

Methods: *The study draws upon relevant international rules, such as the UN Charter and customary international law, as well as recent rulings by the International Court of Justice (ICJ) and the European Court of Human Rights (ECtHR), which can serve as a foundation for developing regulatory frameworks for espionage operations and surveillance activities. The study adopts a doctrinal legal research approach by systematically analysing primary sources of international law, including treaties, customary law principles, and jurisprudence from the ICJ and the ECtHR. It also incorporates a comparative review of state practice and relevant academic commentary to assess whether existing legal norms adequately regulate espionage activities during peacetime.*

Results and Conclusions: *The findings indicate that espionage occupies a legally ambiguous space, particularly concerning the applicability of core principles of non-intervention and state sovereignty—especially in the cyber domain. In parallel, privacy has become enshrined in emerging human rights law, and legal safeguards around state surveillance have been introduced, emphasising proportionality, accountability, and supervision. Still, espionage operates in a highly nuanced legal and ethical territory that is neither wholly abhorrent nor entirely permissible.*

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

This contradiction reflects the ongoing tension between the challenges of balancing national security and the protection of individual rights. While espionage is widely acknowledged as vital to state security, international law does not explicitly ban it despite its potential to violate sovereignty and the principle of non-intervention. However, international law—through its emphasis on territorial integrity and sovereign equality—does not impose certain restraints on espionage activities.

The study concludes that although espionage remains a multifaceted and indispensable component of state actions, it should not violate the principles and laws of sovereignty, human rights, or the broader framework of international law during peacetime. Legal and ethical ambiguity persists, necessitating the development of clearer regulatory frameworks that strike a balance between legitimate intelligence gathering and respect for sovereignty and individual rights. Ultimately, the research underscores that intelligence activities should not be permitted to undermine the stability of the international legal order or erode fundamental human rights protections.

1 INTRODUCTION

Spying is considered one of the oldest professions in the world, or at least the second oldest. From ancient Sumerians to contemporary digital hacking, acquiring secret information has been crucial for states seeking to safeguard or enhance their standing. From Mesopotamian times to the present, the origins of espionage date back over 6,000 years. Even governments from ancient times, such as those in Egypt, Greece, and Rome, are known to have had intelligence services from which modern espionage evolved. In Ancient Egypt, agents were used to spy on people deemed unfaithful to the Pharaohs and to gather information on potential targets of conquest. Similarly, while fighting other city-states, the Greeks would spy on the military might of their opponents.[1] The Romans especially valued spy work, employing many spies who contributed to the creation and sustenance of the most extensive empire in the ancient world.

Amidst the current world order, espionage has undergone a profound change, specifically with the inclusion of what can be considered modern technological enhancements. Modern global Intelligence has over a hundred worldwide intelligence organisations working in developed, developing, and least-developed countries.

States recognise intelligence activities of their own country as necessary for their national security, while denying such practices of other countries as interference in internal affairs. This new age brought new challenges to conventional espionage. Cyber technology has evolved intelligence collection, increasing the speed, visibility, and encapsulation of low-

1 Darien Pun, 'Rethinking Espionage in the Modern Era' (2024) 18(1) Chicago Journal of International Law 353.

intensity operations. Recent releases from the NATO official site confirm that cyberspace is continuously contested, with cyber intrusion attempts on the organisation's premises and malicious cyber events occurring per day on United States military and civilian networks.[2] These intrusions come from more than one hundred countries, proving that intelligence activity nowadays is decentralised worldwide.

Espionage activities were previously limited to wartime intelligence gathering, but now states employ advanced methods during peaceful times to steal secret information from other countries, businesses, and private individuals.[3] Digital technology and increased world connectivity boost the amount and pace of spying operations. NSA surveillance programs of foreign and domestic targets emerged in 2013 through Edward Snowden and Chinese cyberespionage efforts, which were uncovered in 2015.[4] Russia used cyber tools to influence the U.S. presidential election in 2016, proving that espionage extends from general intelligence work to supporting political and economic interests.[5] Espionage operates as a standard tool for statecraft throughout modern international relations.[6] States frequently engage in espionage, yet there are no clear legal rules under international law that explicitly prohibit such activities, particularly in times of peace. This is largely due to the absence of a universal consensus within the international community to outlaw espionage.[7]

While it is often stated that espionage occupies a grey area in international law, allowing it to remain crucial for national security, even though every State publicly condemns spying by others.[8] The absence of a specific treaty prohibiting espionage does not automatically imply a legal void. In fact, international law is composed of various sources, including CIL, general principles of law, and relevant treaties that may implicitly shape the practice of espionage during peacetime.

2 '*Cyber Defence*' (NATO, 30 July 2024) <https://www.nato.int/cps/en/natohq/topics_78170.htm> accessed 15 July 2025.

3 Simon Chesterman, 'Secrets and Lies: Intelligence Activities and the Rule of Law in Times of Crisis' (2006) 28(3) *Michigan Journal of International Law* 553.

4 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, Henry Holt 2014).

5 Heather Stewart, Peter Walker and Julian Borger, 'Russia Spy Poisoning: 23 UK Diplomats Expelled from Moscow' (*BBC*, 17 March 2018) <https://www.bbc.com/news/uk-43440992> accessed 29 January 2025.

6 Jelena Vićić and Erik Gartzke, 'Cyber-Enabled Influence Operations as a "Center of Gravity" in Cyberconflict: The Example of Russian Foreign Interference in the 2016 US Federal Election' (2024) 61(1) Journal of Peace Research 10, doi:10.1177/00223433231225814.

7 Christian Schaller, '*Spies*', *Max Planck Encyclopedia of Public International Law* (2015) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e295> accessed 29 January 2025.

8 Simon Chesterman, '*Secret Intelligence*', *Max Planck Encyclopedia of Public International Law* (2009) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e992> accessed 29 January 2025.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

On the other hand, espionage undermines the sovereignty of States and the principle of non-intervention. However, those States cannot raise the responsibility of States that spy, as espionage itself is not prohibited under International Law, but due to the sovereignty of the States and the principle of non-intervention in the UN Charter, it is possible to constitute the legal basis to raise the responsibility of the spying State.

However, the legality of espionage can be examined through other rules of International law. The legal status of espionage remains measurable, as reflected in international laws, including the United Nations Charter[9] and the Vienna Convention on Diplomatic Relations (1961).[10] State sovereignty principles establish a legal framework for arguments suggesting that espionage activities that violate territorial boundaries or undermine national domestic policy stand against international law. Under the Vienna Convention on Diplomatic Relations framework, diplomatic missions are subject to restrictions on the permissibility of espionage actions.[11] Under Article 41, diplomats must recognise the legal framework of their host state and consistently avoid interfering within its domestic sphere.[12] Many states have employed this principle to remove foreign diplomats suspected of espionage throughout the Cold War era and during recent Russian diplomatic expulsions from Western partners due to spy allegations.[13] States and international bodies utilise existing legal frameworks to assess individual espionage activities, thus determining their legitimacy regarding international law. Despite its acceptance in international relations, espionage exists within an intricate regulatory domain that international diplomacy, politics, and legal systems continually reshape. This study will analyse different legal instruments such as the UN Charter, UNCLOS, and the Chicago Convention to examine the nature of espionage during peacetime, in addition to the legality of espionage in the light of Human Rights and Customary International Law.

2 RESEARCH METHODOLOGY

The research uses the analytical method based on the textual and contextual analysis of legal rules. This method aligns with the present study through the interpretation and analysis of specific provisions of international treaties, such as the United Nations Charter, the United Nations Convention on the Law of the Sea, and the Vienna Convention on Diplomatic Relations, and their application to the issue of espionage. Analysis and interpretation of these legal sources may contribute to determining the legality of espionage. The research

9 *United Nations Charter* (effective 24 October 1945) art 2(7) <https://www.un.org/en/about-us/un-charter> accessed 29 January 2025.

10 *Vienna Convention on Diplomatic Relations (signed 18 April 1961) [1965] UNTS 500/95.*

11 Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (3rd edn, OUP 2013).

12 Geoffrey B Demarest, 'Espionage in International Law' (1996) 24(2) *Denver Journal of International Law and Policy* 321.

13 Chesterman *(n 8)*.

context is also heavily influenced by the inductive method that will be employed to establish a legal framework for espionage by examining international practices that may constitute customary international law. The study will consider the opinions and writings of legal scholars as a subsidiary source of international law by examining jurisprudential trends that support or oppose the legitimacy of espionage in times of peace.

3 LEGALITY OF ESPIONAGE IN LIGHT OF THE PRINCIPLE OF STATE SOVEREIGNTY

The fundamental principle of state sovereignty is a significant defining component that shapes intergovernmental rules regarding espionage activities. According to international law, every state has the autonomy to manage its expenses and maintain control over its territory while being free from outside limitations. Espionage represents a breach of state sovereignty because outside parties perform activities within the exclusive territorial domain of states without their permission.[14] State practice in espionage demonstrates that nations do not always adhere to the established sovereign principles recognised by international law. Pursuing national security through espionage allows states to break the sovereign domain of other countries. The flexibility of sovereignty allows states to conduct espionage actions against each other in order to fulfil their strategic demands. Although espionage operations may destroy diplomatic connections, nations often respond with retaliatory actions. States usually respond to domestic espionage discoveries by forcing embassies to leave the territory while arresting suspected agents and condemning the other state through diplomatic channels.[15] The diplomatic actions demonstrate the struggle between espionage measures and state legal rights protecting national borders. Because international law provides no clear guidelines on espionage, states settle their espionage disputes through diplomatic channels.

According to central tenets of international law, states must never interfere with the internal matters of other nations. Article 2(7) of the United Nations Charter prohibits international intervention in the internal affairs of any state, except in situations where issues of peace or security threaten international stability. The international community generally views espionage activities as banned information-gathering operations. Under the non-interference principle, espionage becomes illegal when state entities steal official secrets or disrupt national domestic issues. Espionage actions targeting political, military, and economic frameworks within a state constitute violations of that state's sovereign position. The United Nations General Assembly repeatedly promotes state non-interference in

14 Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19(5) *American University International Law Review* 1091.

15 Yves Sandoz,·Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff 1987) 561-70.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

domestic matters while protecting nations' sovereignty and territorial independence.[16] States typically accept espionage operations that form part of a national security framework or an intelligence operation. The absence of exact legal mechanisms to address questions regarding espionage makes it hard to implement this principle in practice.

The United Kingdom brought a case against Albania at an international court because it believed Albania violated British rights through dangerous activities such as mining international waters that led to a British ship sinking. The ICJ's ruling, in this case, avoided espionage questions specifically, but their judgment stressed three fundamental principles that protected state sovereignty and blocked both unlawful action and hostility toward states.[17] The Corfu Channel case defines how international law addresses how states protect their sovereignty and security assets, including espionage operations.

The target state considers actions of espionage by another nation within its borders to represent a violation of its sovereign independence. The complex ties between state sovereignty and espionage exist in visible light through U.S. allegations against Cuban espionage targeting U.S. military and intelligence assets.[18] The absence of precise international legal standards leads states to resolve espionage incidents through diplomatic methods instead of trying cases at international courts, even when espionage violates territorial sovereignty.

Therefore, it is clearly important to demonstrate that espionage violates the principle of sovereignty, as a State gains sovereignty either through certain International Conventions or by customary practices as a sovereign state. This concept is also present in Article 1 of the Montevideo Convention (1933), which defines the elements of a state.[19] These elements are considered the basic legal criteria for a State. The text related to the principle of sovereignty was essentially a way to reinforce an already existing customary rule and other conventional rules. Therefore, one of the main consequences that arise from State sovereignty is the principle of non-intervention; thus, the legality of espionage in light of the principle of non-intervention will be discussed below.

16 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (adopted 21 December 1965 UNGA Res 2131 (XX)) <https://digitallibrary.un.org/record/203886> accessed 29 January 2025.

17 *Corfu Channel Case (United Kingdom v Albania)* (ICJ, 9 April 1949) <https://www.icj-cij.org/case/1> accessed 29 January 2025.

18 US House Hearing, 'The President's New Cuba Policy and US National Security, Serial No 114-26' (*US Government Publishing Office*, 26 February 2015) <https://www.govinfo.gov/content/pkg/CHRG-114hhrg93534/html/CHRG-114hhrg93534.htm> accessed 29 January 2025.

19 Convention on Rights and Duties of States (signed 26 December 1933) [1936] UNTS 165/19. Article 1: "The state as a person of international law should possess the following qualifications: a permanent population, a defined territory, government and capacity to enter into relations with the other states."

3.1. Indirect Prohibition under the Principle of Non-intervention

The principle of non-interference is enshrined in Article 2(7) of the United Nations Charter, which restricts all forms of intervention within legal areas protected by state sovereignty.[20] Secret information collection from within another state's territory is a purposeful breach of legal ethics and international standards for maintaining state control over domestic territory.[21] Schaller establishes that espionage operates outside international law prohibitions but regularly clashes with the non-intervention principle.[22] A state's constant execution of intelligence collection activities violates the territorial sovereignty of other states when operating on their lands.

In international law, a contradiction persists since espionage acts as an essential national security tool while undermining established standards for diplomatic relations. Chesterman states that governments allow espionage because such activities are fundamental to diplomacy and military operations, even while developing their counterintelligence capability alongside legal frameworks for sovereignty protection.[23]

Under this principle of non-intervention, a state has the right to defend its sovereignty when espionage interferes with internal decision-making or external relations with other countries. The U-2 incident in the 1960s is a valuable case in this context, demonstrating that peacetime espionage is replete with analytical difficulties. The historical event, in which an American reconnaissance aircraft was shot down over Soviet territory, triggered substantial diplomatic fallout and demonstrated the challenges espionage poses to state sovereignty and international law.

By examining the events of the time, the reactions of diplomats from various countries around the world, and the subsequent legal postures, researchers acquire a modicum of understanding of the practicality of the rules of international law.[24]

This case study underscores the relevance and sensitivity of doctrinal legal research and how specific events can shed light on such overarching concepts as state sovereignty and non-intervention. Similarly, the 2001 EP-3 surveillance aircraft incident between China and the United States illustrates how intelligence operations test state relations through their dual need for airspace boundaries.

20 United Nations Charter (n 9) art 2(7).

21 Karol Ziolkowski, 'Cyber Espionage - New Tendencies in Public International Law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publications 2013) 425.

22 Schaller (n 7).

23 Chesterman *(n 8)*.

24 François Dubuisson and Agatha Verdebout, 'Espionage in International Law', *Oxford Bibliographies Online* (2018) 599, doi:10.1093/obo/9780199796953-0173.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Schaller argues that espionage violations of Article 2(7) of the UN Charter should include unauthorised foreign territory entry or cyber-intrusions, though no explicit prohibition remains.[25] Such an approach supports a broader and more contemporary understanding of what constitutes a breach of sovereignty under international law.

3.1.1. Limits of the Principle of Non-Intervention

Espionage exists without direct restrictions through international law, though multiple legal principles such as the Principle of Non-intervention. This principle is considered a core rule in international law that prohibits states from interfering in the internal or external affairs of other sovereign states unless there is a threat to international peace and security, which is also under the Security Council and not by States themselves. In addition, this principle is also a customary norm, meaning it is accepted as binding by states through consistent practice and with the belief that such practice is legally required.[26]

Espionage challenges the principle of non-intervention by involving a State secretly collecting information inside another state's territory or by gathering intelligence information from the outside using different methods without the other state's consent. Such acts raise legal questions on the extent to which intervention is considered an act of espionage during times of peace, particularly in the context of international affairs, military intelligence, strategic information, and matters concerning national security. Therefore, there is an indirect prohibition on espionage that exists under the principle of non-intervention, prompting the legal inquiry into the extent to which intervention is deemed unlawful, and under what circumstances it may be considered permissible. Determining the legality of espionage during peacetime depends not only on the nature and methods used but also on the degree of coercion, intent to influence, and resulting impact on a state's sovereign decision-making authority.

Therefore, states have created regulatory rules that moderate but do not eliminate espionage capabilities through UNCLOS, the UN Charter, the Chicago Convention, and the Vienna Convention on Diplomatic Relations. The instruments seek to establish unauthorised intelligence gathering as a violation of essential state sovereignty and non-intervention principles. Under the principles of state sovereignty and non-intervention, espionage activities often constitute violations of fundamental state rights. Through Article 2(7) of the United Nations Charter, governments establish a ban on intervening in the domestic affairs of independent states exercising their sovereignty.[27]

25 Michael Schaller, 'Espionage and its Legal Implications: A Comprehensive Analysis of Violations under International Law' (2015) 22(4) Journal of International Law and Diplomacy 152.

26 Niki Aloupi, 'The Right to Non-Intervention and Non-Interference' (2015) 4(3) *Cambridge Journal of International and Comparative Law* 570, doi:10.7574/cjicl.04.03.566.

27 United Nations Charter (n 9) art 2(7).

Through Article 2(7), the United Nations Charter explicitly bans external states from intervening in the domestic matters of sovereign states. The provision is an essential restriction against espionage because it designates it as an illegal activity that disrupts a state's political sovereignty and territorial boundaries. State border operations conducted without consent violate the non-intervention principle because they try to influence domestic and foreign state policies.[28]

3.1.2. Impact of Espionage on the Principle of Non-Intervention

Since espionage often targets sensitive areas, it can be seen as interference. For example, if a state publishes an article disclosing the number of voters expected to participate in elections in another state, the question arises as to whether such an act constitutes interference in that state's internal affairs. If it is indeed considered an intervention, a further inquiry would follow investigating how the publishing state obtained this electoral information.= A similar example can be presented—if State A publishes an article stating that State B possesses three naval fleets, the legality of the act may depend on the source of the information. If such military details are publicly available on State B's official Ministry of Defence website, then under international law, this would not qualify as espionage or unlawful intervention. Publicly accessible data, even when concerning sensitive subjects, does not in itself constitute a violation of the principle of non-intervention.

Furthermore, if espionage is used to pressure a state to act against its will through cyberattacks, blackmail, or disruption, it may qualify as unlawful intervention. On the other hand, if espionage targets a key state function, such as influencing policymaking decisions or altering the outcome of an election, it can be considered a breach of international law. However, this remains a contested area in international law because espionage often occurs in the grey zone between what is legally prohibited and what is internationally tolerated.

In *Nicaragua v. United States*, the International Court of Justice (ICJ) ruled that the U.S. had breached customary international law by supporting the Contra rebels, thereby violating obligations to refrain from using force against another state and infringing on its sovereignty. The court clarified that prohibited intervention under international law does not inherently depend on the use of armed force; rather, interventions employing force represent a clear example of such violations.[29] This ruling established that even non-military interference could contravene the prohibition on intervention. The decision implies that espionage involving the theft of confidential information could itself constitute a prima facie act of intervention, potentially representing a more severe breach of sovereignty than the U.S. actions condemned in the Nicaragua case. Essentially, the

28 Aloupi (n 26) 576.

29 *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (ICJ, 27 June 1986) para 147 <https://www.icj-cij.org/case/70> accessed 29 January 2025.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

judgment broadened the scope of prohibited intervention to include covert or non-forceful acts that undermine a state's sovereign rights.[30]

Unauthorised surveillance inside a foreign country's borders violates this principle of sovereignty. Through its provisions in the Vienna Convention on Diplomatic Relations (1961), states receive safeguards against espionage that defend their sovereign rights.[31] Ziolkowski confirms that, although international law does not forbid it, espionage is restricted through diplomatic countermeasures, such as the persona non grata principle, which allows for the expulsion of spies.[32]

International law protects states from external interference, ensuring they retain full control over their internal affairs. According to the United Nations Charter under Article 2(7), the principle protects state sovereignty by prohibiting intervention from one state into another's domestic affairs.[33] Espionage legal practices are ambiguous because intelligence collection activities are conducted through covert actions within another state's territory without the consent of that state. As the boundary of legal intervention through espionage is unclear, there are complex technical distinctions to be made about what constitutes prohibited practices. National security institutions often develop traditional espionage operations to gather essential information about politics, military assets, and the economy. Espionage is also conducted through surveillance and wiretapping, as well as covert tasks to achieve state internal monitoring goals.[34] There is no formal prohibition against intelligence-gathering activities, which creates legal ambiguities under international law. However, these operations are actively violating fundamental rules about the independence of states and their right to remain uninvolved in the affairs of others. Spying, through its practice, disrupts the target nation's political stability and social norms, providing an indirect means to influence the way the state government operates. The choice of political information as an intelligence objective to change policies and political structures reduces a state's ability to make independent decisions. The International Court of Justice affirmed this view in its 1986 decision in the Nicaragua case, in which sovereign decision interference was classified as a violation of state independence.[35] The court ruled that nations have exclusive power over their political and domestic space and cannot be subjected to unauthorised intelligence activities.

The debate about espionage aimed at human rights defence reviews the subtle aspects of this practice. By exposing international human rights violations, these military operations place human dignity above traditional national security aims. Others argue that foreign

30 Jared Beim, 'Enforcing a Prohibition on International Espionage' (2018) 18(2) *Chicago Journal of International Law* 654.
31 *Vienna Convention on Diplomatic Relations* (n 10).
32 Ziolkowski (n 21) 464.
33 United Nations Charter (n 9) art 2(7).
34 Sandoz, Swinarski and Zimmermann (n 15) 561-70.
35 *Military and Paramilitary Activities in and against Nicaragua* (n 29).

surveillance operations should be permitted if the International Covenant on Civil and Political Rights (ICCPR) allows for monitoring of fundamental human rights violations.[36]

However, this position is highly controversial. Critics contend that any collection of any Intelligence, even in humanitarian circumstances, violates the state's sovereignty. They argue that the point of interference maintained by the United Nations and the international community also covers human rights concerns. Their grounds for establishing a non-intervention doctrine, namely the excessive erosion of state sovereignty through espionage and human rights violations, should directly relate to the outcome.[37] It also shows how human rights under international law can be interpreted as not interfering with states' sovereign rights. It is also a question of broader questions about how much national sovereignty should be sacrificed to global humanitarian responsibility in the new millennium, as intelligence gathering nets become more sophisticated.

Espionage activities may be a potential justification for serving broad humanitarian goals that can prevent or stop the identification of human rights abuses. State approval is essential to conduct such operations since their implementation without consent breaks international law principles. Intelligence operations protecting human rights face criticism for their involuntary intrusion against international legal norms concerning states' right to remain independent.

Ultimately, the non-intervention principle, combined with the use of spies, remains a relatively legal affair and opportunistic. While the UN Charter and other state practices contain guidelines for state conduct in international relations, they lack precise and enforceable standards to evaluate intelligence-gathering activities. As the global landscape becomes increasingly interconnected through information sharing and cross-border surveillance, the boundaries of prohibited interference continue to shift—redefining sovereignty in the new complex manoeuvres of super-intelligence.

3.2. Indirect Prohibition in the light of the conventional rules

The analysis of espionage during peacetime requires examining relevant international conventions. While these conventions do not explicitly establish a legal basis for espionage, they may be interpreted in accordance with the means of treaty interpretation outlined in Articles 31 and 32 of the 1969 Vienna Convention on the Law of Treaties (VCLT), which could provide significant legal limitations on such activities. This interpretive methodology is crucial for maintaining the international legal order and fostering peaceful international relations.

36 Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 192-5.

37 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States (n 16).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Article 31 VCLT states that treaties "shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[38] Supplementary means of interpretation under Article 32 VCLT, including preparatory work (*travaux préparatoires*) and the circumstances of a treaty's conclusion, further clarify the meaning when interpretation under Article 31 leaves it ambiguous or obscure, or leads to a manifestly absurd or unreasonable result.[39]

Based on these means, it is evident that espionage during peacetime, widely condemned by States for its potential to undermine international stability, is implicitly restricted by conventional rules. This section examines significant provisions in certain conventions, such as Article 19(2)(c) of the United Nations Convention on the Law of the Sea (UNCLOS), the 1944 Chicago Convention on International Civil Aviation, and Article 3(1)(d) of the Vienna Convention on Diplomatic Relations.

3.2.1. Impact of Espionage on the Maritime Sovereignty

State sovereignty receives protection under several international conventions that establish restrictions on espionage. Surveillance activities, as defined by UNCLOS standards, remain restricted to state territorial waters due to explicit permissions outlined in the United Nations Convention on the Law of the Sea (UNCLOS).[40] The ordinary meaning of Article 19(2)(c) UNCLOS explicitly prohibits foreign vessels exercising the right of innocent passage if they engage in "any act aimed at collecting information to the prejudice of the defence or security of the coastal State."[41] According to international law, these regulations prevent intelligence ships from monitoring territories through their states' 12-nautical-mile border unless proven otherwise. Thus, confirming that state sovereignty becomes jeopardised when espionage occurs.

Article 19(2)(c) of UNCLOS clearly prohibits vessels from passing through the territorial sea and engaging in any act aimed at collecting information of the coastal state; such an act is considered unlawful, and the vessel would be given direct orders to leave the territorial sea of a sovereign state.

Espionage during peacetime is often carried out under the guise of innocent passage, such as intelligence gathering, the acquisition of military data, or the interception of sensitive communication. It directly violates the principle of sovereignty over a State's maritime space, and furthermore, it represents an indirect breach of the principle of non-intervention. The fact that the right of innocent passage is subject to limitations clearly indicates that espionage falls into a grey area of international law.

38 Vienna Convention on the Law of Treaties (signed 23 May 1969) [1987] UNTS 1155/331, art 31.
39 ibid, art 32.
40 Chesterman *(n 8)*.
41 United Nations Convention on the Law of the Sea (signed 10 December1982) [1998] UNTS 1833/3, art 19(2)(c).

For instance, if a surveillance or naval intelligence vessel passes through the territorial sea of another state and actively gathers strategic military information, such as surveillance of coastal defence systems, this would constitute a violation of Article 19(2)(c), even if no weapons are used. The pretence of innocent passage becomes irrelevant if the underlying activity compromises the coastal state's national defence. A hypothetical example would be a ship from State A sailing through State B's territorial waters while collecting encrypted military transmissions from coastal installations. Even if the data were passively gathered without entering restricted zones, the activity would still breach Article 19(2)(c) due to its adverse impact on State B's security.

However, a key question arises when information gathering occurs outside a state's territorial sea, particularly within its Exclusive Economic Zone (EZZ). This issue is exemplified by the 2009 USNS Impeccable incident, in which a U.S. military surveillance vessel operating near China's southern coast in the EEZ was accused of conducting unlawful intelligence operations.[42] Although the EEZ lies beyond the territorial sea and does not confer full sovereignty to the coastal state, the diplomatic fallout that followed between China and the USA illustrates the seriousness with which maritime espionage is viewed by coastal states as an act of intervention.

The United States maintained that its actions were consistent with the freedoms of navigation and overflight guaranteed under the United Nations Convention on the Law of the Sea (UNCLOS), particularly Articles 58 and 87. However, China objected on the basis that such activities violated its sovereign rights and constituted a threat to its national security.[43]

Although the EEZ is not subject to full sovereignty in the same manner as the territorial sea, coastal states retain sovereign rights for the purposes of exploring and exploiting natural resources and may also regulate certain economic and environmental activities. The ambiguity lies in whether foreign military intelligence operations, while not explicitly prohibited under UNCLOS, can be interpreted as infringing on these sovereign rights or amounting to intervention in internal affairs. To answer this uncertainty, the UNCLOS does not regulate the legality of peacetime maritime espionage in these zones. However, in an indirect way, such actions are a violation of the principle of sovereignty, especially when national security interests are implicated.

42 Carlyle A Thayer, 'The United States and Chinese Assertiveness in the South China Sea' (2010) 6(2) Security Challenges 69.

43 Raul Pedrozo, 'Preserving Navigational Rights and Freedoms: The Right to Conduct Military Activities in China's Exclusive Economic Zone' (2010) 9(1) *Chinese Journal of International Law* 13-7.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

3.2.2. Impact of Espionage on the Aerial Sovereignty

According to Article 1 of the Chicago Convention on International Civil Aviation (1944), states possess "complete and exclusive sovereignty over the airspace above its territory." [44] This foundational principle affirms that every State enjoys complete and exclusive sovereignty over the airspace above its territory. As such, no foreign aircraft can enter the airspace of another country without its permission. If any contracting state violates an article of this convention during peacetime, this act may constitute a breach of the principle of sovereignty and the terms of the agreement.

This article thus establishes a clear legal framework requiring prior authorisation for entry into a sovereign state's airspace. Acts of aerial espionage—such as unauthorised surveillance, intelligence collection by aircraft, even if flying at high altitudes—are considered an indirect prohibition of the principle of sovereignty.

This principle is often cited in legal challenges involving unauthorised aerial espionage. Two events illustrate the methods states employ in response to perceived violations of this principle: the 1960 U-2 incident and the 2023 Chinese spy balloon incident.

The U-2 incident stands as a landmark case in interpreting the impact of espionage on aerial sovereignty. In 1960, a United States aircraft was shot down by the Soviet forces while flying above the Soviet Union on a high altitude conducting aerial surveillance.[45] Legally, the U-2 incident constituted a clear violation of the Soviet Union's airspace under Article 1 of the Chicago Convention and under customary international law, even if it was conducted at high altitudes. Although the Chicago Convention does not directly address military aircraft,[46] however, the principle of sovereignty over national airspace is internationally recognised and binding on all aircraft, whether civil or state.[47]

This incident illustrates the consequences of unauthorised aerial surveillance and reinforces the principle that even non-aggressive flights conducted for intelligence purposes can constitute unlawful intervention under international law.[48] While the International Court of Justice (ICJ) has not directly ruled on aerial espionage, the logic applied in cases such as Nicaragua v United States supports the view that covert surveillance which violates a state's territorial sovereignty may also infringe the non-intervention principle.[49]

44 Convention on International Civil Aviation (signed 7 December 1944) [1948] UNTS 15/295, art 1.

45 Raymond L Garthoff, *Reflections on the Cuban Missile Crisis* (2nd edn, Brookings Institution Press 1989) 4. See also: Gregory W Pedlow and Donald E Welzenbach, *The CIA and the U-2 Program, 1954-1974* (History Staff Center for the Study of Intelligence CIA 1998).

46 Convention on International Civil Aviation (n 44) art 3(a).

47 Bin Cheng, *The Law of International Air Transport* (Stevens & Sons Ltd; Oceana Publications Inc 1962) 131; Ian Brownlie, *Principles of Public International Law* (7th edn, OUP 2008) 289.

48 Ramesh Thakur, *The United Nations, Peace and Security: From Collective Security to the Responsibility to Protect* (CUP 2006) 108.

49 *Military and Paramilitary Activities in and against Nicaragua (n 29)* para 205.

Similarly, the 2023 Chinese spy balloon incident raised significant political concerns. The United States alleged that a high-altitude balloon operated by the Chinese government entered its airspace, hovering over several states, including sensitive military areas, without prior permission.[50] The Chinese spy balloon incident indicates a violation of the Chicago Convention and the aerial sovereignty of a State, regardless of whether a spy balloon qualifies as an aircraft or not.[51] The international legal ambiguities surrounding the legal status of aerial objects highlight the Convention's limitations, particularly in addressing emerging technologies and distinguishing between national airspace and outer space.[52]

Technology has led Chesterman to observe that international intelligence operations routinely use aerial and space-based reconnaissance even though these practices remain without a legal framework.[53] In analysing the two incidents, there is no clear treaty that can regulate espionage during peacetime in light of aerial sovereignty incidents. Without clear legal regulation, aerial espionage remains a grey area in international law—widely regarded as a breach of state rights when conducted without consent and to the prejudice of national security.

3.2.3. Impact of Espionage on Diplomatic Relations

The legal framework established by the Vienna Convention on Diplomatic Relations (1961) raises special issues related to diplomatic espionage operations. Foreign embassies must fulfil their mission by employing legal methods to assess the conditions of the receiving state and then report their findings to their respective home governments, as per Article 3(1)(d) of the agreement. This diplomatic function requires lawful actions to conduct intelligence activities in accordance with current legal provisions. The difficulty arises from identifying proper boundaries in intelligence operations, as representatives traditionally use their official roles for hidden collection activities.[54]

Under the Vienna Convention, procedural actions exist to respond to diplomatic privilege exploitation that can validate espionage activities. The convention allows states to identify foreign diplomats who conduct intelligence operations outside acceptable limits and then issue a declaration of persona non grata.[55] Observations from the Tehran Hostages Case

50 Kevin Fang, Priyanka Shah and Benjamin Rosen, 'A Right to Spy? The Legality and Morality of Espionage' (*Just Security*, 15 March 2023) <https://www.justsecurity.org/85486/a-right-to-spy-the-legality-and-morality-of-espionage/> accessed 29 January 2025.

51 Look up article: Batuhan Betin, 'Skies, Spies, and Scientific Surveys – The Legal Aspects of Chinese Unmanned Balloon Flight Over American Territory' (*EJIL:Talk!*, 6 March 2023) <https://www.ejiltalk.org/skies-spies-and-scientific-surveys-the-legal-aspects-of-chinese-unmanned-balloon-flight-over-american-territory/> accessed 29 January 2025.

52 Dean N Reinhardt, '*The Vertical Limit of State Sovereignty*' (LLM thesis, McGill University Montreal (Quebec) 2005).

53 Chesterman *(n 8)*.

54 *Vienna Convention on Diplomatic Relations* (n 10) art 3(1)(d).

55 ibid, art 9(1).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

(1980) exposed an embattled relationship between the diplomatic shield and espionage activities because Iran accused the U.S. embassy in Tehran of carrying out intelligence actions against its government.[56] Despite refraining from addressing espionage charges, the International Court of Justice declared that states facing suspicions of foreign diplomats' illegal activities still benefit from Vienna Convention protections.[57] Military attachés carry out intelligence tasks that require them to operate under terms defined by the accepting nation's legal framework.[58] International law remains uncertain about the status of diplomatic espionage because states traditionally handle violations through diplomatic methods rather than legal court systems, following many Cold War-era expulsions of diplomats.[59]

Furthermore, analysing espionage under international law requires special attention to recognising diplomatic immunity. Under Articles 41 and 42 of the Vienna Convention on Diplomatic Relations (1961), diplomatic agents are granted protection from criminal prosecution by their host country in relation to their official duties. The Vienna Convention does not provide diplomatic protection regarding espionage activities, which are considered beyond the scope of legitimate diplomacy.[60]

This distinction was notably illustrated in the 2018 expulsion of Russian diplomats from the United Kingdom, following the attempted assassination of a former Russian intelligence officer.[61] British authorities invoked the diplomatic expulsion mechanism to respond to what they characterised as a violation of their sovereignty.

International relations gain their legal framework from state practices that evaluate espionage conduct versus diplomatic immunity while resolving their inherent tensions. International legal systems provide no definitive rules on the prohibition of espionage, so states must decide independently whether espionage activities are in accordance with their laws. Such a complex paradox of the international community's approach to espionage is reflected in the fact that states tend to conduct intelligence operations while simultaneously condemning the same activity within their borders.

This duality manifests in a range of diplomatic responses, including the expulsion of ambassadors, surveillance of foreign diplomats, and the management of incidents involving the capture of spies. It also extends to the routine practice of clandestine intelligence gathering carried out under the cover of diplomatic missions. By definition, intelligence gathering involves violating domestic law or territorial sovereignty by agents engaging in

56 *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (ICJ, *24 May 1980*) <https://www.icj-cij.org/en/case/64> accessed 29 January 2025.
57 ibid, para 86.
58 Chesterman *(n 8)*.
59 Demarest (n 12).
60 Vienna Convention on Diplomatic Relations (n 10) arts 41, 42.
61 Stewart, Walker and Borger (n 5).

the clandestine acquisition and collection of information that falls within the domains of domestic law or territorial sovereignty across borders.

Despite this, states continue to guard against their legal status to espionage, while also knowing its critical importance to national defence and foreign policy advancement—an issue that remains ambiguously unclarified.[62] In practice, nations typically resolve espionage incidents diplomatically through diplomatic expulsions and formal protests. The international community condones espionage not only through a legal lack of enforcement or even a refusal to punish it as a war crime but, in fact, through its tacit acknowledgement of espionage as a prerequisite to the state's functioning. As a result, espionage operations persist even when they contravene fundamental principles of international law, sustained by a form of global tolerance grounded in practical necessity.

This gap between legal norms and state practice underscores the divergence between the formal legal framework and the reality of national security operations. While the Vienna Convention on Diplomatic Relations (1961) regulates diplomatic privileges and immunity, it does not legitimise espionage. Diplomatic missions maintain reporting duties within host states, yet the Vienna Convention defines their intelligence-gathering activities as lawful procedures.[63]

Historically, diplomatic missions served as convenient cover for covert intelligence activities while performing duty-related functions. The practice of states conducting espionage through diplomatic missions remains limited by international legal provisions that allow host states to eject undercover spies using the persona non grata principle. The diplomatic community has established a solid international standard that prohibits the improper exploitation of diplomatic immunity for intelligence operations.

4 LEGALITY OF ESPIONAGE IN LIGHT OF THE HUMAN RIGHTS LAW

Human rights, including privacy protection, face growing threats as states intensify their oversight of citizens. Intelligence agencies conduct bulk data intercepts of communications to watch persons, yet typically lack a sufficient legal basis for their activities. The European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) established that surveillance programs reduced freedom of speech and organisational contact while intensifying privacy dangers.[64]

The practice of state surveillance has evolved to include bulk data collection from telecommunication networks, which has become one of the main espionage developments in recent times. Worldwide national security operations now heavily rely on state

62 Aloupi (n 26) 575.

63 Vienna Convention on Diplomatic Relations (n 10).

64 Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55(2) *Virginia Journal of International Law* 310.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

surveillance, which governments deploy to combat terrorism, cyber threats, and various other national security threats. The expansion of surveillance technology creates substantial privacy protection violations in opposition to global human rights law protections.[65] Under international human rights law, the right to privacy is a fundamental human right, according to both ECtHR and ICCPR. Article 17 of the ICCPR states that, "No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor unlawful attacks on their honour and reputation". Article 8 of the ECHR safeguards individuals from arbitrary interference with their private life, family, home, and correspondence.[66] The rising practice of population-wide bulk communications data collection makes it harder to uphold privacy protections established by law.

Digital technology advances have enabled intelligence agencies to process unprecedented volumes of data with maximum efficiency. However, state power today faces additional concerns through bulk data collection—facilitated by artificial intelligence and cyber surveillance tools—has made espionage operations far broader than before.[67]

According to judicial decisions, mass data retention tactics have faced outsized privacy implications, including multiple rulings such as *Big Brother Watch and Others v. U.K.* (ECtHR, 2021) and *Schrems II* (CJEU, 2020).[68] Stricter oversight mechanisms coupled with activity constraints represent essential measures that courts have identified to stop the abuse of intelligence operations.

While technology remains vital to national security—particularly in addressing threats and terrorism—the upcoming challenge requires regulatory bodies to establish procedures that safeguard intelligence collection from exceeding its necessity and human rights boundaries.

Prior judicial decisions established that courts provide better protection to content data than metadata. Therefore, the line separating content data from metadata has become increasingly difficult to distinguish.[69] The CJEU, in *Digital Rights Ireland* (2014) and *Tele2 Sverige* (2016), determined that metadata can reveal information comparable in sensitivity to content data, and thus must be subject to strong safeguards during investigation procedures.[70] This position reaffirmed by the ECtHR in *Big Brother Watch and Others v. U.K.*,

65 ibid 295.
66 ibid.
67 Schaller (n 7).
68 *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 2021) para 314 <https://hudoc.echr.coe.int/fre?i=001-210077> accessed 29 January 2025; *Facebook Ireland and Schrems* C-311/18 (CJEU, 16 July 2020) <https://curia.europa.eu/juris/liste.jsf?num=C-311/18> accessed 29 January 2025.
69 Deeks (n 64) 311.
70 *Digital Rights Ireland and Seitlinger and Others* C-293/12, C-594/12 (CJEU, 8 April 2014) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293> accessed 29 January 2025; *Tele2 Sverige* C-203/15, C-698/15 (CJEU, 21 December 2016) <https://curia.europa.eu/juris/liste.jsf?num=C-203/15> accessed 29 January 2025.

where the Court stressed that the bulk interception of communications data needs detailed oversight measures.[71]

At times, states engage in data collection in a random and unselective manner, leading to an apparent overlap between information gathering and the act of espionage. This raises a fundamental question: to what extent does data collection infringe upon the right to privacy under human rights law? The following sections will aim to clarify and analyse how mass surveillance and bulk data collection can result in interference with human rights law. In addition to focusing on the growing use of surveillance technologies, which can come with conflict with the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). A key legal standard used by international bodies and courts—the necessity and proportionality test—will then be analysed to evaluate whether restraints on privacy can be justified as espionage practices or protection of national security.

4.1. Mass Surveillance and Bulk Data Collection and Privacy Interference

The surveillance techniques employed in bulk data collection pose significant consequences for privacy rights through their ability to process extensive records from surveillance. International human rights law dictates that bulk surveillance must meet both the requirement standards and the proportionality requirements, yet this approach often lacks specificity in practice.[72]

In *Carpenter v United States* (2018), the Supreme Court of the United States decided that warrantless collection of location data constituted a serious intrusion on privacy[73] and required judicial authorisation.[74] Similarly, in *Zakharov v. Russia* (2015), the ECtHR determined that Russian surveillance legislation was insufficient to protect against misuse and failed to ensure effective judicial oversight.[75] These rulings underscore a broader concern: big data analytics and artificial intelligence technology have enabled intelligence agencies to create sophisticated individual profiles, thus expanding privacy violation concerns.[76]

The extent to which surveillance tracks movements and behaviours, combined with a lack of regulatory boundaries, raises worries about its compatibility with fundamental human rights. Public judicial powers require basic legal rules for surveillance activities and independent control mechanisms to protect the rights of victims who have suffered violations of their rights.

71 *Big Brother Watch and Others v United Kingdom* (n 68) para 314.
72 Deeks (n 64) 311.
73 *Carpenter v United States* [2018] 585 US 296; 138 S Ct 2206, 2219.
74 ibid.
75 *Zakharov v Russia App no 47143/06* (ECtHR, 4 December 2015) <https://hudoc.echr.coe.int/fre?i=001-159324> accessed 29 January 2025.
76 Deeks (n 64) 308.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

A key example of this legal tension is the invalidation of the EU-U.S. Privacy Shield 2020 by the CJEU. The decision was based on the findings that U.S. intelligence agencies conducted excessive surveillance that denied EU citizens adequate legal protections.[77]

Building a framework of what constitutes or does not constitute a legal precedent through court rulings has been established to balance national security needs with individual privacy protections. Through the cooperation of international organisations and the work of judicial bodies, new legal standards for surveillance practices have evolved. As states pursue legitimate security interests, they continue to set the standards by which they wish state-sponsored intelligence operations to operate in accordance with the rule of international human rights legislation. This is an area in the legal landscape where surveillance practices can be regulated in a way that balances collective security interests with individual interests. These principles strike a balance between the various needs, enabling states to protect health information in a manner that maintains security while respecting privacy rights. While surveillance is an inherently indispensable shield when it comes to safeguarding national defence, it must be carried out in a way that also protects fundamental human rights.

4.2. Balancing Espionage and Privacy Rights: The Necessity and Proportionality Test

International human rights laws require that restrictions on fundamental rights demonstrate necessity and proportionality for authorised aims, including national security. States frequently justify espionage or surveillance as essential to safeguarding national security; however, such activities impact the right to privacy. To reconcile this tension or conflict, human rights frameworks require restrictions on privacy to satisfy the necessity and proportionality test, ensuring espionage activities remain lawful only when strictly aligned with legitimate security aims and accompanied by robust safeguards.

The necessity criterion requires that surveillance measures be essential to achieving an important objective—such as countering terrorism—and that no less intrusive alternatives exist. The proportionality test refers to a surveillance program that does not disproportionately harm individual privacy compared to the public benefit. Submerged surveillance remains subject to precise court supervision to fulfil necessary principles according to court decisions.

This was affirmed in *Schrems II* (CJEU, 2020) where the Court invalidated the EU-U.S. Privacy Shield agreement on the grounds that U.S. intelligence agencies improperly collected EU citizens' data without adequate available remedies.[78] The decision established that effective intelligence acquisition needs to maintain proper equilibrium with personal privacy safeguarding methods.[79]

77 *Facebook Ireland and Schrems* (n 68) .
78 *ibid.*
79 Deeks (n 64) 311.

Similarly, in *Big Brother Watch*, the ECtHR required bulk surveillance programs to implement specific legal frameworks with autonomous authorisation systems and effective remedy procedures.[80] The absence of such safeguards constituted a violation of Article 8 of the European Convention on Human Rights, which protects the right to privacy.

Therefore, there must be a proportionate relationship between the act of espionage and its consequences. If the harm to privacy is minimal and the benefit to public security is substantial, the proportionality test may be fulfilled under international legal standards. For example, it may be necessary to conduct surveillance in a specific area if there is credible information indicating that a bomb has been planted in a school—this would constitute a legitimate security objective. However, conducting surveillance merely because there is a possibility of data theft from an agricultural institution in a certain region would not meet the threshold of necessity. In such a case, the activity would more accurately be characterised as espionage rather than lawful surveillance, and it would not be legal under human rights law.

5 LEGALITY OF ESPIONAGE IN LIGHT OF CUSTOMARY INTERNATIONAL LAW

When examined through the principles of international customary law, the unauthorised collection of secrets for political or military gain—defined as espionage—sparks multiple legal uncertainties. These concerns centre around the legality of espionage under international customary law (CIL). States establish international customary law through consistent and widespread global practices that derive legal obligations from those practices. The principal issue regarding espionage during peacetime under international law is determining what constitutes prohibited conduct under legal standards and whether such acts receive worldwide condemnation.

Customary International Law (CIL) is a fundamental source of international law that emerges through key elements: consistent, systematic, and concurrent state practice, with the belief that states are obligated to adhere to such practice by legal norms. Unlike treaties, CIL is not written and emerges gradually through the state's actions and opinions.[81] Contrary to the view that CIL is outdated or a legal technique of the past, it is not a stagnant legal regime, as some people perceive it. Although the formation of the CIL rule calls for robust evidence of continued State practice, the law remains flexible. Indeed, CIL has not been relegated to the periphery of international law; it remains one of its essential components, capable of further refinement and clarification.

80 *Big Brother Watch and Others v United Kingdom* (n 68).

81 Panos Merkouris, 'Interpreting Customary International Law: You'll Never Walk Alone' in Panos Merkouris, Jörg Kammerhofer, and Noora Arajärvi (eds), *The Theory, Practice, and Interpretation of Customary International Law* (The Rules of Interpretation of Customary International Law, CUP 2022) 347, doi:10.1017/9781009025416.017.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Determining whether espionage is permissible under CIL requires a nuanced analysis of the frequency of state intelligence activities, coupled with states' official and military responses to espionage cases. Opinio juris regarding the permissibility of such activities may evolve alongside emerging international legal standards.[82] As legal opinions constantly evolve, the legal status of espionage under CIL can also change in response to contemporary state practices and legal perceptions. Therefore, the interpretation is never static but remains open to ongoing reassessment.

This section examines espionage law based on international customary principles, utilising analysis from state practice, domestic legislation and judicial proceedings. For centuries, states have employed intelligence gathering as a key component of their national security strategy to gain strategic advantages. Despite widespread state engagement in this practice, international law continues to grapple with its legal implications. At the core of the debate lies the question of whether espionage constitutes a violation of international law, and whether a customary international rule prohibiting it exists.

CIL is derived from two primary criteria: state practice and opinio juris. State practice refers to the regular standard activities performed by states, while opinio juris represents the legal belief states hold towards particular acts. Although the prevalence of espionage supports the existence of a widespread practice,[83] there remains uncertainty over the status of its actual prohibition.

Many states criminalise espionage under domestic law, while others have not adopted any legislative restrictions. This raises the question: to what extent can espionage be considered unlawful under customary international law (CIL)? As is well established, CIL has two core elements: state practice and the belief that such state practice is legally obligatory.

If a substantial majority of states—say, 150—criminalise espionage within their domestic legal systems, this may be interpreted as strong evidence of consistent and general state practice, suggesting that espionage is widely regarded as legally impermissible under customary international law.[84] However, the situation is complicated by the fact that a significant number of other states—such as 50 or more—remain silent or acquiescent in formally objecting to espionage activities, despite taking preventive measures against the act of espionage.[85] Therefore, the legality of espionage remains ambiguous, falling into a grey area under customary international law.

Espionage is often considered an indispensable instrument for states to achieve their objectives in national security and international foreign relations activities. The common occurrence of state espionage practices and the uncertain status under international law

82 ibid.

83 Peter Malanczuk, *Akehurst's Modern Introduction to International Law* (7th edn, Routledge 2002).

84 Malcolm N Shaw, *International Law* (9th edn, CUP 2021) 74-7.

85 Ashley Deeks, 'The Legal Framework for Intelligence Collection' (2016) 38(2) *Harvard National Security Journal* 357.

present analytical challenges for determining their acceptability under CIL. Despite being criminalised in many domestic legal systems, espionage is neither explicitly prohibited nor expressly permitted under international law. As such, it occupies a legal grey area—widely practised, yet not formally codified as legal or illegal at the international level. Consequently, while espionage is tolerated as a matter of state practice, its acceptability as a legal norm under customary international law remains unresolved, largely due to the lack of consistent opinio juris among states.

Under national laws, many states impose criminal sanctions on espionage to protect vital state information and national security. For example, the U.S. official statutes for espionage date back to 1917 and originate from the Espionage Act of 1917, which prohibits unauthorised access to or sharing of national defence information.[86] Under the UK's Official Secrets Act of 1989, individuals are punished for sharing information without authorisation related to national security topics, sensitive activities, and international relations matters.[87] Execution of espionage and collection of Intelligence remains essential through state laws establishing national sovereignty regulations. Although espionage is subject to criminal penalties under national laws, this legal fact does not establish the existence of an international rule against espionage in customary international law.[88] Legislation under national law typically defines laws specific to national state legal systems, yet fails to represent established standards within international law frameworks. Each state may engage in espionage without facing international consequences, particularly when national security or foreign policy interests are at stake.

International treaties also offer little clarity. No specific treaty prohibits espionage during peacetime. International humanitarian law, as established through the Geneva Conventions and their Additional Protocols, addresses espionage primarily in the context of armed conflict. During peacetime, the United Nations Charter prohibits interference in the internal affairs of states, but it does not explicitly outlaw espionage.[89] A specialised international framework to govern espionage remains absent, further complicating customary international law analysis regarding their prohibition.

Nevertheless, certain judicial rulings and legal instruments offer indirect constraints. While no international convention expressly bans espionage, its legality is often assessed through generalised concepts, such as state independence, protection for diplomatic representatives, and restrictions on harmful state-to-state behaviours.

86 *18 US Code, ch 37, pt 1 Espionage and Censorship, § 792–799.*

87 *Official Secrets Act* 1989, c 6 (UK).

88 Asaf Lubin, 'Espionage as a Sovereign Right under International Law and Its Limits' (2016) 24(3) ILSA Quarterly 24.

89 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States (n 16); United Nations Charter (n 9).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

The legal framework for espionage under international customary law exists without explicit prohibition but is subject to indirect restrictions through legal instruments that protect state sovereignty and territorial integrity. These indirect limitations can be found in instruments such as the UN Charter, the Vienna Convention on Diplomatic Relations (1961), and the United Nations Convention on the Law of the Sea (UNCLOS). However, none of these treaties explicitly prohibit espionage.

Customary international law is further shaped by judicial decisions of the International Court of Justice. For example, in *Nicaragua v. United States* (1986), the ICJ held that America's secret operations against Nicaragua were deemed a breach of customary international law, which protects the principle of non-intervention. This case illustrates how espionage, when it constitutes interference in another state's domestic affairs, can breach international norms, even though espionage is not formally outlawed.

Under the United Nations Convention on the Law of the Sea (UNCLOS), Article 19(2)(c) prohibits foreign vessels from engaging in intelligence gathering within the territorial waters (12 nautical miles) of a coastal state. This provision reinforces the protection of the sovereignty of coastal states.[90] The application of espionage laws to the maritime sphere reaffirms the more general principle that sovereignty over borders remains with states and that such intelligence gathering, even at sea, is not to invade the sovereignty of a state.

Thus, while espionage is not categorically prohibited under customary international law, it is indirectly constrained through various legal instruments and norms that prioritise states' sovereignty. Its legality often hinges on how states perceive and apply international legal principles in their jurisdiction.

In parallel, courts such as the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) have emphasised that mass surveillance requires detailed protections for individual privacy, even when used for national defence. The Court of Justice of the European Union ruled that gathering bulk communications data infringed upon privacy rights as minimal legal protection could not adequately safeguard such data collection.[91] In *Big Brother Watch and Others v. U.K.* (2021), the ECtHR ruled that surveillance programs require effective oversight to protect against misuse and uphold necessity constraints.[92] Governments require the necessity criterion alongside proportionality principles to regulate their surveillance practices. Under IHL, any restriction of privacy must have a valid purpose, be necessary for achieving that aim, and be proportionate to the objective pursued.

90 United Nations Convention on the Law of the Sea (n 41).
91 Deeks (n 64) 308.
92 *Big Brother Watch and Others v United Kingdom* (n 68).

Any data collection approach that fails to establish legal grounds for specific purposes will not align with these essential requirements. This case contains an essential principle of necessity and proportionality. In *Carpenter v. United States* (2018), the U.S. Supreme Court expanded privacy protections by holding that location data deserved similar constitutional protections as communication content. Intelligence agencies have enhanced privacy violations through Artificial Intelligence and big data analytics by developing comprehensive profiles of individuals through their communication and activity patterns.[93] These observational tools that process entire datasets allow governments to perform surveillance that might result in extreme privacy invasions. A greater volume of collected data combined with improvements in data complexity leads to higher threats against users' privacy rights.

6 CONCLUSIONS

Espionage remains a grey area within international law. While states categorically consider intelligence collection necessary for security, many of these operations are contrary to the most basic notions of sovereignty, privacy rights and territorial integrity. Although surveillance activities occur with equal frequency in states, such as the abuse of state sovereignty and borders, this tension in international relations arises from the ambiguous legal status of surveillance activities. Nevertheless, states argue that these operations are required to fulfil security needs and, as a result, these operations almost always violate non-intervention standards and territorial integrity. These breaches of international law cannot be justified on their own by justifications of national security.

The current international legal regime neither adequately prohibits nor explicitly permits espionage, revealing a critical gap in governance. This regulator vacuum underscores the urgent need for a more coherent and normative legal approach—whether through clearer treaty-based regulation or the development of customary norms—to address the evolving complexities of modern intelligence operations.

This research contributes to the understanding of espionage by highlighting the fluidity of international legal order and the pragmatism of state behaviour. It offers a complex model for understanding information gathering beyond the legal and ethical binary oppositions and emphasises the importance of adapting legal and diplomatic strategies in response to global integration. As technological capabilities continue to evolve and global interconnectedness intensifies, future research must create more refined legal definitions for cyber intelligence and discuss the ethical implications of new forms of surveillance, in addition to examining the effects of intelligence practices on diplomatic relations in the long run.

93 *Carpenter v United States* (n 73).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

This paper has examined the interplay between espionage and the principle of state sovereignty, particularly through the lens of Article 2(7) of the UN Charter, which prohibits intervention in matters essentially within the domestic jurisdiction of any state. Ultimately, the evolving nature of espionage demands that international law adapt through flexible yet principled frameworks. These must uphold the core values of sovereignty and human rights, while providing legal clarity to govern intelligence activities in a way that promotes transparency, accountability, and peaceful coexistence in the international system. States typically accept espionage operations that form part of a national security framework or an intelligence operation. However, the absence of exact legal mechanisms to address questions regarding espionage makes it hard to implement this principle in practice. The world of espionage remains dynamic and complex, compelling a reassessment of conventional understanding of sovereignty, security, and cooperation within the international system.

With the world constantly evolving, intelligence practices must be analysed with the sophistication and flexibility required in the contemporary world. Espionage is an activity in evolution, and the modernisation of this reality demands an adequate new legal system that reconciles essential security requirements with fundamental freedoms at the national and individual levels. Civilised or not, espionage will still be a natural means of statecraft. However, it must be controlled by setting clear legal boundaries to protect the territorial integrity and critical infrastructure.

Espionage should therefore not be left entirely unregulated. Instead, a dual regulatory approach at both the national and international levels is necessary. Such an approach must establish clear legal boundaries while remaining adaptable to technological advancement. Regulatory frameworks must prioritise the protection of territorial integrity, privacy, and fundamental human rights, ensuring intelligence practices are conducted within ethical and legal constraints.

In conclusion, while the complete regulation of espionage may be unrealistic given its covert nature and strategic importance, international collaboration can facilitate the development of shared norms and minimum international standards. These should aim to reconcile state interests with the core principles of sovereignty, non-intervention, and human rights. As technological capabilities advance, legal systems must evolve in tandem to continue providing sufficient international protection of national sovereignty, privacy, and human rights—particularly in times of peace.

REFERENCES

1. Aloupi N, 'The Right to Non-Intervention and Non-Interference' (2015) 4(3) *Cambridge Journal of International and Comparative Law* 566, doi:10.7574/cjicl.04.03.566.
2. Baker CD, 'Tolerance of International Espionage: A Functional Approach' (2004) 19(5) *American University International Law Review* 1091.
3. Beim J, 'Enforcing a Prohibition on International Espionage' (2018) 18(2) *Chicago Journal of International Law* 647.
4. Brownlie I, *Principles of Public International Law* (7th edn, OUP 2008).
5. Cheng B, *The Law of International Air Transport* (Stevens & Sons Ltd; Oceana Publications Inc 1962).
6. Chesterman S, *'Secret Intelligence'*, *Max Planck Encyclopedia of Public International Law* (2009) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e992> accessed 29 January 2025.
7. Chesterman S, 'Secrets and Lies: Intelligence Activities and the Rule of Law in Times of Crisis' (2006) 28(3) *Michigan Journal of International Law* 553.
8. Deeks A, 'An International Legal Framework for Surveillance' (2015) 55(2) *Virginia Journal of International Law* 291.
9. Deeks A, 'The Legal Framework for Intelligence Collection' (2016) 38(2) Harvard National Security Journal 346.
10. Demarest GB, 'Espionage in International Law' (1996) 24(2) *Denver Journal of International Law and Policy* 321.
11. Dubuisson F and Verdebout A, 'Espionage in International Law', *Oxford Bibliographies Online* (2018) 599, doi:10.1093/obo/9780199796953-0173.
12. Fang K, Shah P and Rosen B, 'A Right to Spy? The Legality and Morality of Espionage' (*Just Security*, 15 March 2023) <https://www.justsecurity.org/85486/a-right-to-spy-the-legality-and-morality-of-espionage> accessed 29 January 2025.
13. Fleck D (ed), *The Handbook of International Humanitarian Law* (3rd edn, OUP 2013).
14. Garthoff RL, *Reflections on the Cuban Missile Crisis* (2nd edn, Brookings Institution Press 1989).
15. Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, Henry Holt 2014).
16. Lubin A, 'Espionage as a Sovereign Right under International Law and Its Limits' (2016) 24(3) ILSA Quarterly 22.
17. Malanczuk P, *Akehurst's Modern Introduction to International Law* (7th edn, Routledge 2002).

18. Merkouris P, 'Interpreting Customary International Law: You'll Never Walk Alone' in Panos Merkouris, Jörg Kammerhofer, and Noora Arajärvi (eds), *The Theory, Practice, and Interpretation of Customary International Law* (The Rules of Interpretation of Customary International Law, CUP 2022) 347, doi:10.1017/9781009025416.017.
19. Pedlow GW and Welzenbach DE, *The CIA and the U-2 Program, 1954-1974* (History Staff Center for the Study of Intelligence CIA 1998).
20. Pedrozo R, 'Preserving Navigational Rights and Freedoms: The Right to Conduct Military Activities in China's Exclusive Economic Zone' (2010) 9(1) *Chinese Journal of International Law* 9.
21. Pun D, 'Rethinking Espionage in the Modern Era' (2024) 18(1) Chicago Journal of International Law 353.
22. Reinhardt DN, '*The Vertical Limit of State Sovereignty*' (LLM thesis, McGill University Montreal (Quebec) 2005).
23. Sandoz Y, Swinarski C and Zimmermann B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff 1987).
24. Schaller C, '*Spies*', *Max Planck Encyclopedia of Public International Law* (2015) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e295> accessed 29 January 2025.
25. Schaller M, 'Espionage and its Legal Implications: A Comprehensive Analysis of Violations under International Law' (2015) 22(4) Journal of International Law and Diplomacy 152.
26. Schmitt MN (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).
27. Shaw MN, *International Law* (9th edn, CUP 2021).
28. Thakur R, *The United Nations, Peace and Security: From Collective Security to the Responsibility to Protect* (CUP 2006).
29. Thayer CA, 'The United States and Chinese Assertiveness in the South China Sea' (2010) 6(2) Security Challenges 69.
30. Vićić J and Gartzke E, 'Cyber-Enabled Influence Operations as a "Center of Gravity" in Cyberconflict: The Example of Russian Foreign Interference in the 2016 US Federal Election' (2024) 61(1) Journal of Peace Research 10, doi:10.1177/00223433231225814.
31. Ziolkowski K, 'Cyber Espionage - New Tendencies in Public International Law' in Ziolkowski K (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publications 2013) 425.

AUTHORS INFORMATION

Fawaz Najem*
PhD Researcher in Public Law, University of Sharjah, Sharjah, United Arab of Emirates
U23101493@sharjah.ac.ae
https://orcid.org/0009-0007-5623-8973
Corresponding author, responsible for writing the original draft, the methodology, and the formal analysis.

Abdelnaser Aljahani
Associate Professor of International Law, University of Sharjah, Sharjah, United Arab of Emirates
aaljahani@sharjah.ac.ae
https://orcid.org/0000-0003-0937-6824
Co-author, responsible for conceptualizing, reviewing, and supervising the original draft.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declares that their opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

Managing editor – Mag. Bohdana Zahrebelna. **English Editor** – Julie Bold.
Ukrainian language editor: Lilia Hartman.

ABOUT THIS ARTICLE

Cite this article
Najem F and Aljahani A, 'The Legality of Espionage in Peacetime' (2025) 8(3) Access to Justice in Eastern Europe 1-32 <https://doi.org/10.33327/AJEE-18-8.3-a000118> Published Online 05 Aug 2025

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

DOI: https://doi.org/10.33327/AJEE-18-8.3-a000118

Keywords: *Espionage, State Sovereignty, Non-Intervention, Cyber-Espionage, Privacy Rights, Surveillance.*

DETAILS FOR PUBLICATION

Date of submission: 03 May 2025
Date of acceptance: 22 Jun 2025
Online First publication: 05 Aug 2025
Whether the manuscript was fast tracked? - Yes
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ЗАКОННІСТЬ ШПИГУНСТВА В МИРНИЙ ЧАС

Фаваз Наджем* та Абдельнасер Альджахані

АНОТАЦІЯ

Вступ. *У цій дослідницькій роботі розглядається законність шпигунства в мирний час згідно з нормами міжнародного права. Для вирішення цього питання в статті увага зосереджується на низці відповідних норм міжнародного права, включно з зобов'язанням поважати суверенітет інших держав та дотриманням принципу невтручання. Хоча шпигунство є давнім інструментом державного управління, необхідним для гарантування національної безпеки, воно займає невизначене правове становище. Міжнародно-правові норми, зокрема Статут ООН та звичаєве міжнародне право, встановлюють такі зобов'язання, як повага до державного суверенітету та дотримання принципу невтручання, які часто ставить під сумнів шпигунська діяльність. Зростання сучасних можливостей спостереження, особливо в кіберсфері, ще більше ускладнюють правові та етичні межі шпигунства.*

Методи. *Дослідження ґрунтується на відповідних міжнародних нормах, таких як Статут ООН та норми звичаєвого права, а також на нещодавніх рішеннях Міжнародного Суду ООН (МС ООН) та Європейського суду з прав людини (ЄСПЛ), які можуть слугувати основою для розробки нормативно-правової бази для шпигунських операцій та діяльності зі спостереження. У статті застосовано доктринальний підхід до правового дослідження за допомогою системного аналізу первинних джерел міжнародного права, зокрема договорів, принципів звичаєвого права та судової практики Міжнародного Суду ООН (МС ООН) та Європейського суду з прав людини (ЄСПЛ). У роботі також було здійснено порівняльний огляд державної практики та відповідних академічних коментарів для оцінки того, чи адекватно чинні правові норми регулюють шпигунську діяльність у мирний час.*

Результати та висновки. *Результати роботи свідчать про те, що шпигунство займає юридично неоднозначне місце, особливо щодо застосування основних принципів невтручання та державного суверенітету в сучасному шпигунстві, особливо в кіберсфері. Окрім того, конфіденційність дедалі більше закріплюється у сфері прав людини, а також запроваджено правові гарантії контролю за державним спостереженням із наголосом на принципах пропорційності, підзвітності та нагляду. Тим не менш, шпигунство діє в дуже тонкій правовій та етичній площині, яка не є ні повністю забороненою, ні повністю дозволеною.*

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Ця суперечність відображає постійну напругу між викликами балансування національної безпеки та захисту прав окремої людини. Хоча шпигунство широко визнається життєво важливим для безпеки держави, міжнародне право прямо його не забороняє, незважаючи на потенціал порушення суверенітету та принципу невтручання. Однак міжнародне право, акцентуючи увагу на принципах невтручання, територіальної цілісності та суверенної рівності, не накладає чітких обмежень на шпигунську діяльність.

У дослідженні було зроблено висновок, що хоча шпигунство розглядається як багатогранний та невід'ємний компонент дій держави, воно не повинно порушувати принципи та закони суверенітету, прав людини та/або ширші засади міжнародного права в мирний час. Правова та етична неоднозначність досі існує, тож це вимагає розробки більш чіткої нормативно-правової бази, яка б забезпечувала баланс між законним збором розвідувальних даних та повагою до суверенітету та прав людини. Зрештою, у дослідженні наголошено на тому, що розвідувальна діяльність не повинна підривати стабільність міжнародного правопорядку або руйнувати захист основних прав людини.

Ключові слова: *шпигунство, державний суверенітет, невтручання, кібершпигунство, права на конфіденційність, спостереження.*