



Reinterpretation of Article 27 of the 1961 Vienna Convention on the Cyber Interception of Diplomatic Communications

^{1st} Muhammad Rayyan Arifin*, ^{2nd} Andi Muhammad Mappatempa Salim, ^{3rd} Irsyad Dhahri, ^{4th} Fernando Ignasio Wijaya, ^{5th} Melwan Saputra

¹ Universitas Negeri Makassar, Indonesia,

² Universitas Negeri Makassar, Indonesia,

³ Universitas Negeri Makassar, Indonesia,

⁴ Universitas Negeri Makassar, Indonesia,

⁵ Universitas Negeri Makassar, Indonesia

*email: muhrayyanarifin25@gmail.com

Keywords:

*Diplomatic Law;
Article 27 VCDR;
Diplomatic
Communications;
Cyber
Interception;
Evolutive
Interpretation*

ABSTRACT

*The development of digital technology has transformed diplomatic communication from physical media into electronic networks that are increasingly vulnerable to cyber interception. This study examines the relevance of Article 27 of the 1961 Vienna Convention on Diplomatic Relations (VCDR) in protecting electronic diplomatic communications and formulates a normative reinterpretation suited to developments in the cyber environment. It employs a normative juridical method using treaty, conceptual, historical, and case approaches. The analysis is based on Articles 31 and 32 of the 1969 Vienna Convention on the Law of Treaties, decisions of the International Court of Justice, the Tallinn Manual 2.0, UN GGE and OEWG documents, and relevant State practice. The findings show that Article 27(1) and (2) can be applied to electronic communications through evolutive interpretation of the terms “free communication,” “all appropriate means,” and “official correspondence.” The study formulates four principles of reinterpretation: medium neutrality, location independence, layered obligations, and the protection of the confidentiality and availability of communications. Cyber interception targeting the official communications of a diplomatic mission is more appropriately analyzed under diplomatic law as *lex specialis*. For Indonesia, the findings underscore the importance of harmonizing wiretapping and cybersecurity policies, strengthening the technical protection of diplomatic communications, and formulating a clear national position on the application of diplomatic law in cyberspace.*

1. INTRODUCTION

Diplomacy is, in essence, an activity that depends heavily on communication. A diplomatic mission performs the functions of representing the sending State, protecting the interests of the State and its nationals, negotiating with the government of the receiving State, ascertaining by lawful means the conditions and developments in the receiving State, and promoting friendly relations between States. These functions are set out in Article 3(1) of the 1961 *Vienna Convention on Diplomatic Relations* (VCDR). They can be performed effectively only if a diplomatic mission is able to communicate

freely, securely, and without interception by third parties with the government of the sending State and with its other representations. For this reason, the International Law Commission (ILC) identified freedom of communication as one of the generally recognized freedoms essential to the performance of a diplomatic mission's functions (ILC, 1958).

The guarantee of diplomatic communication was subsequently codified in Article 27 of the VCDR. Article 27(1) requires the receiving State to permit and protect free communication on the part of the mission for all official purposes. It also allows the mission to employ "all appropriate means," including diplomatic couriers and messages in code or cipher, provided that the installation and use of a wireless transmitter require the consent of the receiving State. Article 27(2) further provides that the official correspondence of the mission is inviolable and covers all correspondence relating to the mission and its functions (United Nations, 1961).

The problem arises because the VCDR was drafted in the early 1960s, when diplomatic communication was still dominated by letters, telegrams, coded messages, and diplomatic couriers. Technological developments have since transformed the mission's official communications through electronic mail, internet networks, cloud computing services, and digital infrastructure that spans multiple jurisdictions. This transformation has widened the risk of interception through network penetration, the compromise of devices or servers, and access to digital service providers. As a result, the protection of diplomatic communications no longer concerns physical security alone but also the confidentiality and continuity of communications in the cyber environment.

The literature on diplomatic law shows that electronic surveillance has long been a source of difficulty in the application of the VCDR. Denza (2025) treats freedom of communication and the inviolability of official correspondence as fundamental to the effectiveness of a diplomatic mission's functions. This indicates that the protection of communications concerns not merely the medium used but the need to safeguard the freedom, security, and confidentiality of a mission's official communications.

The interception of communications between States has direct relevance for Indonesia. In November 2013, the disclosure of Edward Snowden's documents concerning alleged Australian intelligence surveillance of the communications of President Susilo Bambang Yudhoyono in 2009 prompted an Indonesian diplomatic response consisting of the recall of its ambassador for consultations and a formal request for an explanation from Australia (ABC News, 2013; Al Jazeera, 2013a, 2013b). Although this case does not directly demonstrate a violation of Article 27 of the VCDR, because it did not specifically target the official correspondence of a diplomatic mission, the episode illustrates the political and legal consequences of surveillance of inter-State communications and the importance of clarifying the protection of diplomatic communications in the digital environment.

Another relevant development appears in *Timor-Leste v. Australia* in 2014, in which the International Court of Justice ordered Australia to ensure that the seized

documents and electronic data belonging to Timor-Leste's legal adviser would not be used to the detriment of Timor-Leste while the proceedings were pending (International Court of Justice, 2014). Although the case was not based directly on the VCDR, the order shows that the confidentiality of State documents and communications may constitute a legal interest deserving international protection.

These technological changes raise a normative problem because Article 27 of the VCDR does not expressly mention the internet, electronic mail, digital encryption, cloud computing services, or cyber interception. At the same time, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* has sought to connect diplomatic law with cyber activities. Chapter 7 of the *Tallinn Manual 2.0* addresses diplomatic and consular law in the cyber context. It contains Rule 39 on the inviolability of premises housing cyber infrastructure, Rule 40 on the duty to protect cyber infrastructure, and Rule 41 on the inviolability of electronic archives, documents, and correspondence. Jensen (2017) explains that Rule 41 applies the protection of diplomatic and consular law to the cyber context. The Manual's discussion of these rules also touches on electronic surveillance by third States of diplomatic communications and on the particular challenges involved in the duty to protect cyber communications from interception.

At the level of the United Nations, developments in international norms likewise show a recognition that international law continues to apply to State activities in cyberspace. The report of the United Nations Group of Governmental Experts (UN GGE) affirmed that international law, in particular the Charter of the United Nations, applies to the use of information and communications technologies by States (United Nations General Assembly, 2015). A similar conclusion was reaffirmed in the report of the *Open-ended Working Group* (OEWG), which stated that existing obligations under international law continue to apply to State activities relating to information and communications technologies (United Nations General Assembly, 2021). Nevertheless, neither forum has offered a specific explanation of how the particular rules of diplomatic law, especially Article 27 of the VCDR, should be applied to the interception of digital communications.

This situation reveals a gap between the general recognition that international law applies in cyberspace and certainty about how the special rules of diplomatic law are to be applied. The issue is further complicated because international law does not contain a general prohibition on all forms of cyber espionage in peacetime. The *Tallinn Manual 2.0* explains that cyber espionage is not in itself always contrary to international law, but that the methods used to carry out such operations may violate other international legal obligations (Schmitt, 2017). In the context of diplomatic communications, Article 27 of the VCDR therefore has the potential to operate as a special rule (*lex specialis*) that provides a more specific legal standard for the interception of a mission's official communications.

In the Indonesian context, the issue has likewise not received adequate attention. Indonesian legal scholarship on diplomatic communication has focused largely on the diplomatic bag, the abuse of diplomatic immunity, and conventional wiretapping. Mangku (2010), for example, examines the alleged wiretapping of the Embassy of the Republic of Indonesia in Yangon under the VCDR and treats it as a violation of diplomatic immunity. That study is important as a foundation, but the development of internet-based communications, cloud storage, and remote interception raises new problems that cannot be fully explained by an approach centered on conventional wiretapping.

Based on these developments, three research gaps can be identified. First, there remains a need for an analysis that systematically applies the rules of interpretation in Articles 31 and 32 of the 1969 *Vienna Convention on the Law of Treaties* (VCLT) to determine whether Article 27(1) and (2) of the VCDR can extend to electronic communications and cyber interception. Second, the relationship between the specific protection afforded by diplomatic law and the general debate on espionage and sovereignty in cyberspace has not been explicitly addressed in much of the literature. Third, studies in Indonesia remain limited in linking the protection of diplomatic communications to the development of digital technology and to national policy needs.

In light of these gaps, this study poses three research questions. First, how can Article 27(1) and (2) of the VCDR be interpreted under Articles 31 and 32 of the VCLT so as to protect electronic diplomatic communications? Second, what is the position of Article 27 of the VCDR as *lex specialis* in determining the legal protection and State obligations concerning the interception of diplomatic communications in cyberspace? Third, how can principles for reinterpreting Article 27 of the VCDR be formulated to address developments in digital communication technology, and what are their implications for Indonesia's policy on protecting diplomatic communications?

In line with these research questions, this study aims to analyze the scope of protection that Article 27 of the VCDR affords to electronic diplomatic communications through an evolutive interpretive approach; to examine the position of diplomatic law as *lex specialis* in addressing cyber interception, together with the State obligations it generates; and to formulate principles of normative reinterpretation that are relevant to developments in digital technology and to Indonesia's national policy needs. The analysis rests on the argument that the terms "free communication," "all appropriate means," and "official correspondence" in Article 27 are generic and functional in character, which allows legal protection to be applied to contemporary communication media without altering the substance of the VCDR.

The novelty of this study lies in developing a framework for reinterpreting Article 27 of the VCDR through four principles: medium neutrality, location independence, layered obligations, and the protection of the confidentiality and availability of communications. Unlike approaches that emphasize the protection of conventional means of communication, this study treats the official function of

diplomatic communication as the basis for determining legal protection, including when communication takes place through cross-border digital infrastructure. The framework also provides a normative basis for identifying State obligations and for formulating policy implications for the protection of diplomatic communications in Indonesia.

2. RESEARCH METHOD

This study employs a normative juridical, or doctrinal, method that treats norms of international law as the principal object of analysis. It focuses on the interpretation and application of Article 27 of the VCDR to electronic diplomatic communications and the threat of cyber interception. Accordingly, the study does not aim to measure the empirical behavior of diplomatic actors; rather, it seeks to construct a legal argument grounded in treaty provisions, international judicial decisions, official documents of international organizations, State practice, and relevant doctrine.

Four approaches are used in an integrated manner. First, the statute and treaty approach is used to examine the 1961 VCDR, particularly Articles 24, 27, 40, and 41, as well as the 1969 VCLT, especially Articles 31 and 32 on the rules of treaty interpretation. In the national legal context, the study also examines Law No. 1 of 1982 on the ratification of the Vienna Conventions on Diplomatic Relations and on Consular Relations and Law No. 37 of 1999 on Foreign Relations.

Second, the conceptual approach is used to analyze the concepts of freedom of diplomatic communication, the inviolability of official correspondence, the theory of functional necessity, *due diligence*, sovereignty in cyberspace, *lex specialis*, and evolutive interpretation of treaty terms. This approach is used to determine whether the protection of diplomatic communications depends on the physical form of the medium or on the function of the communication in carrying out the tasks of a diplomatic mission.

Third, the historical approach is used to trace the origins of the norm in Article 27 of the VCDR through the *Draft Articles on Diplomatic Intercourse and Immunities with Commentaries* prepared by the International Law Commission in 1958. The historical approach serves as a supplementary means of interpretation for understanding the original purpose of protecting diplomatic communications and the relationship between freedom of communication and the effective performance of the mission's functions.

Fourth, the case approach is used to examine the decisions and orders of the International Court of Justice and relevant State practice. The decisions analyzed include *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)* (1980), *Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)* (2009), and *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)* (2014 and 2015). These cases were selected because they bear on diplomatic inviolability, the evolutive interpretation of treaty terms, and the protection of the confidentiality of State documents and communications.

The legal materials in this study are divided into primary, secondary, and tertiary materials. Primary materials comprise the 1961 VCDR, the 1969 VCLT, decisions and orders of the International Court of Justice, official documents of the United Nations Group of Governmental Experts (UN GGE) and the Open-ended Working Group (OEWG), and relevant Indonesian legislation. Secondary materials include books, scholarly journal articles, academic commentaries, and doctrinal works on diplomatic law and cyber law, including the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Tertiary materials are used to assist in searching for and clarifying concepts, among them the *Max Planck Encyclopedia of Public International Law* and the *Cyber Law Toolkit*.

The legal materials were collected through library research and online searches of legal documents. Sources were selected for their direct relevance to three areas of analysis: the protection of diplomatic communications, the interpretation of international treaties, and the application of international law in cyberspace. Official documents, international decisions, and legislation were given priority as primary sources, while doctrine and scholarly literature were used to strengthen the construction of the argument and to map academic debates.

The analysis was conducted qualitatively in three stages. The first stage was descriptive analysis, which identified and mapped the normative structure of Article 27 of the VCDR and related provisions. The second stage was interpretive analysis, applying the rules of Article 31 of the VCLT, which provide for interpretation in good faith in accordance with the ordinary meaning of the terms, their context, the object and purpose of the treaty, subsequent practice, and other relevant rules of international law, and Article 32 of the VCLT as a supplementary means of interpretation. The third stage was prescriptive analysis, which formulated a reinterpretation of Article 27 to determine the standard of protection for diplomatic communications against cyber interception and its implications for Indonesia.

Evolutionary interpretation is applied in a limited manner to the generic terms in Article 27, especially the phrases “free communication,” “all appropriate means,” and “official correspondence.” This method is used because the VCDR is a treaty intended to operate over the long term and because developments in communication technology could not be fully foreseen when the Convention was drafted. However, evolutionary interpretation is not used to alter provisions that are explicitly physical in character, such as the concept of the diplomatic bag, but to test the extent to which the functional protection in Article 27(1) and (2) can encompass electronic communications.

The State practice discussed in this study, including the 2013 disclosure of Indonesian–Australian communications surveillance and the alleged wiretapping of the Indonesian Embassy in Yangon, is used as an illustration for assessing State reactions and the normative relevance of Article 27, not as factual proof that each alleged intelligence operation has been legally established. This limitation is necessary because information on intelligence operations and cyber interception generally derives from

public disclosures, the media, or documents that are not always officially confirmed by the States concerned.

This study has limitations because it relies on legal sources and information that are publicly available and does not use interviews with diplomats, government officials, or cybersecurity institutions. Accordingly, its findings are doctrinal and prescriptive in nature and are intended to build a legal argument that can be further tested through developments in State practice, national position statements, and the future formation of international norms.

3. RESULTS AND DISCUSSION

3.1. Anatomy of Article 27 and Its Related Provisions

The analysis shows that applying Article 27 of the VCDR to electronic communications does not require the creation of a new norm. This protection can be constructed from the normative structure of Article 27 itself when it is interpreted under the rules in Articles 31 and 32 of the VCLT. The crucial point lies in the open and functional character of Article 27's wording, particularly the phrases "free communication," "all appropriate means," and "official correspondence."

Article 27(1) contains four elements. The first is the dual obligation of the receiving State to permit and to *protect* free communication. The first verb gives rise to a negative obligation not to obstruct, whereas the second gives rise to a positive obligation to act. The second element is the scope of purposes, namely all official purposes. The third element is the scope of means, namely all appropriate means, with couriers and messages in code or cipher mentioned as examples. The fourth element is the conditional exception that a wireless transmitter may be installed and used only with the consent of the receiving State.

The same is true of Article 27(2). The provision does not define official correspondence by its physical form but by its connection to "the mission and its functions." The decisive variable in determining protection is therefore not whether the communication takes the form of a letter, a telegram, an e-mail, an instant message, or a data packet, but whether it relates to the performance of the mission's official functions. This definition is important because it is built on function rather than on medium.

This reading is strengthened when Article 27 is placed alongside other provisions of the VCDR. Article 24 provides that the archives and documents of the mission are inviolable "at any time and wherever they may be." Article 40(3) requires third States to accord official communications in transit, including messages in code or cipher, the same freedom and protection as the receiving State is bound to accord. Article 41 obliges members of the mission to respect the laws of the receiving State, not to interfere in its internal affairs, and not to use the mission premises in any manner incompatible with the functions of the mission. Together, these provisions form a single system of protection: freedom of communication, inviolability of materials, protection of location, and limits on abuse.

These findings show that the protection of diplomatic communications in the VCDR is built on function rather than on any particular technology. Consequently, the shift from analog to digital communication does not in itself remove its legal protection.

3.2. Evolutive Interpretation of the Generic Terms in Article 27

Evolutive interpretation is relevant because the VCDR is an international treaty designed to apply over the long term and uses generic terms. Under Article 31(1) of the VCLT, a treaty must be interpreted in good faith in accordance with the ordinary meaning of its terms, in their context, and in the light of its object and purpose.

The phrases “free communication” and “all appropriate means” are open-ended. The drafters did not compile a closed list of means of communication but gave examples (couriers, cipher) within an open formulation. The definition of official correspondence is likewise function-based. The reference to “messages in code or cipher” shows that the drafters understood the confidentiality of a message’s content as the core of the protection rather than as a side effect. The wireless-transmitter clause shows that the drafters confronted the new technology of their day and chose to regulate it through a consent requirement rather than excluding it from the scope of Article 27. In other words, technological change within the same functional category was already anticipated by the text.

The object and purpose of the VCDR further support this reading. The theory of functional necessity reflected in the Preamble to the VCDR requires an interpretation that preserves the ability of missions to work efficiently. A reading that protects a sealed letter but leaves an e-mail with identical content open to anyone able to intercept it would defeat that purpose. Such a result would be absurd, and Article 32 of the VCLT permits recourse to supplementary means of interpretation to avoid it.

In *Costa Rica v. Nicaragua*, the International Court of Justice explained that the use of generic terms in a treaty intended to apply for a long period can support an interpretation that follows the evolving meaning of those terms (International Court of Justice, 2009). Nevertheless, this judgment does not directly prove that the parties to the VCDR intended the meaning of Article 27 to evolve. A more relevant historical basis is found in the commentary of the International Law Commission (ILC, 1958) on draft Article 25, which became the basis for the regulation of freedom of communication in Article 27 of the VCDR. The ILC affirmed that freedom of communication is an essential element in the performance of a diplomatic mission’s functions and that a mission may use all appropriate means of communication for official purposes. The commentary also indicates that developments in communication practice were taken into account in formulating the norm, including changes in communication patterns among diplomatic representations in different countries. In addition, the ILC affirmed that official correspondence remains protected even when it is not carried in a diplomatic bag. Under Article 32 of the VCLT, the ILC commentary, as part of the preparatory work of the Convention, may be used as a supplementary means of interpretation to confirm that the protection of diplomatic communications has a

functional orientation and is not entirely confined to the means of communication known when the Convention was drafted (ILC, 1958).

This argument is consistent with Article 31(1) of the VCLT, which requires a treaty to be interpreted according to the ordinary meaning of its terms, in their context, and in the light of its object and purpose. However, as Arato (2010) explains, evolutive interpretation must be distinguished from interpretation based on subsequent practice, because they are distinct interpretive techniques that do not always lead to the same conclusion. In the context of Article 31(3)(b) of the VCLT, States' use of digital communication technology does not in itself prove the existence of subsequent practice showing the parties' agreement on the interpretation of Article 27. Therefore, in the absence of evidence of State practice meeting that requirement, the evolutive interpretation advanced in this study rests primarily on the generic character of the phrase "all appropriate means," on the functional purpose of protecting diplomatic communications, and on the 1958 ILC commentary as a supplementary means of interpretation under Article 32 of the VCLT. The application of Article 27 to electronic communications is thus a normatively defensible interpretive construction, not a claim that all States parties have agreed to extend the scope of protection for diplomatic communications in cyberspace.

Even so, evolutive interpretation has limits. It must not be *contra legem*, that is, contrary to the express text. An important distinction must be drawn here. Paragraphs 3 and 4 define the diplomatic bag as a package bearing visible external marks of its character, so a "digital bag" cannot be constructed by stretching the word "bag." Reinterpretation, however, does not require this. The protection of electronic communications can be derived from paragraph 1 on free communication and paragraph 2 on official correspondence, neither of which is tied to a physical form.

3.3. Cyber Interception as a Matter of Diplomatic Inviolability

Recognizing that electronic communications fall within the scope of Article 27 has a further consequence: the interception of a mission's official communications must be analyzed as a matter of diplomatic inviolability, not merely as a general question of espionage.

In international law, the status of peacetime espionage remains debated. The *Tallinn Manual 2.0* indicates that cyber espionage is not automatically prohibited by any single general norm of international law. However, the absence of a general prohibition does not mean that all methods of espionage are permitted. An intelligence operation may still contravene international law if the manner in which it is carried out violates a specific applicable rule.

For diplomatic communications, Article 27 of the VCDR is that specific rule. Where the target of an operation is the official correspondence of a diplomatic mission, the interception must be assessed under the inviolability attaching to that communication. The principal legal question is therefore not whether "espionage" is

abstractly permitted, but whether a State is entitled to access communications that the treaty declares inviolable.

This approach provides a more precise legal basis than relying on the concept of cyber sovereignty alone. International debate continues over whether sovereignty in cyberspace is a primary rule of law whose violation independently gives rise to State responsibility or merely a principle underlying other rules. Article 27 does not depend on resolving that debate, because it imposes a more specific treaty obligation with respect to diplomatic communications.

This study therefore finds a shift in the *locus* of analysis: when a cyber operation targets the official communications of a diplomatic mission, the primary framework should be not the general law of espionage but diplomatic law as *lex specialis*.

3.4. The Problem of Data Location, Metadata, and Third-Party Infrastructure

Applying Article 27 in cyberspace becomes more complex when communications are not physically located in the embassy building. Diplomatic communications may be stored in data centers or cloud computing systems in other countries, while the infrastructure is operated by private companies.

Article 24 of the VCDR provides that the archives and documents of the mission are inviolable “at any time and wherever they may be.” This wording supports the argument that the protection of a mission’s official materials does not depend wholly on their physical location.

If server location were made a condition of protection, the use of cloud computing could in practice eliminate inviolability merely because data moves from a local server to a data center in a third State. Such a result would contradict the functional nature of diplomatic protection.

However, the involvement of private companies raises a different jurisdictional problem. Digital service providers are subject to the law of the place where the company or the server is located. A State may require providers to hand over data through domestic legal process. In such circumstances, a conflict may arise between the provider’s domestic obligations and the State’s international obligations with respect to diplomatic communications.

For that reason, the principle of inviolability does not remove the sending State’s need to build a technical security architecture. Legal protection and technical security should be understood as two complementary layers.

A more difficult question concerns metadata. Article 27(2) uses the term “correspondence,” which has traditionally been associated with the content of a communication. Metadata such as the identities of the sender and recipient, the time of communication, network addresses, the frequency of message exchange, or device location do not necessarily contain the substance of a message.

In the digital environment, however, the aggregation of metadata can reveal highly sensitive patterns of diplomatic relationships and activities. The frequency of communication alone, for example, can be used to map the intensity of relations between an embassy and a particular actor.

This study therefore proposes a functional test. Metadata should be protected where its collection or processing enables others to obtain information about diplomatic patterns, substance, or relationships in a way that undermines the confidentiality and effectiveness of the mission's functions.

It must be emphasized that this construction is a doctrinal proposal. Neither the drafts of the VCDR nor the available State practice provides a final answer for every type of metadata. The status of metadata therefore marks one of the limits of the reinterpretation developed in this study.

3.5. The Structure of State Obligations in Protecting Cyber Diplomatic Communications

The analysis of Article 27 shows that the protection of digital diplomatic communications generates a structure of obligations that is not unitary. These obligations involve the receiving State, third States, and the sending State in different capacities.

3.5.1. Negative Obligations of the Receiving State

The first obligation is the prohibition on the receiving State directly interfering with a mission's official communications. Interception, extraction of message content, unauthorized storage, or the use of official communications for the receiving State's own interests contravenes the principle of inviolability when directed at communications within the scope of Article 27.

This prohibition applies to the acts of State organs regardless of their institutional form. Thus, the status of an intelligence agency, law-enforcement body, regulator, or administrative institution does not alter the State's international obligations. Under the law of State responsibility, the conduct of State organs is generally attributable to the State.

Further implications arise for domestic rules on wiretapping and data access. National provisions that generally permit wiretapping for particular purposes cannot automatically override the inviolability of diplomatic communications. Nor can the clause in Article 27 on the receiving State's consent to the use of wireless transmitters be interpreted as authority to access the content of communications. That consent relates to the use of devices or frequencies, not to the removal of the inviolability of correspondence.

3.5.2. Positive Obligations of the Receiving State

The phrase "permit and protect" indicates that Article 27 does not stop at an obligation of non-interference. The receiving State also bears a positive obligation to take relevant protective measures.

The logic of this positive obligation is consistent with the judgment of the International Court of Justice in *United States Diplomatic and Consular Staff in Tehran*. The Court treated the receiving State not only as a party that must refrain from violating a diplomatic mission but also as one under an obligation to take steps to protect the mission from the acts of others.

In the cyber context, this obligation should not be understood as an obligation of result requiring the State to guarantee that an attack never occurs. Cyber threats involve a high degree of technical complexity and difficulty of attribution. The obligation is therefore better understood as a *due diligence* obligation, that is, an obligation to take reasonable measures in light of the State's knowledge, capacity, level of risk, and capabilities.

Such measures may include dealing with illegal interception devices, responding to reports of threats against foreign representations' communications, protecting relevant telecommunications infrastructure, and coordinating with electronic system operators where there are indications of an attack on diplomatic communications.

This study does not, however, assume that Article 27 sets detailed technical standards for cybersecurity. What can be derived normatively is the existence of a duty of protection, while the concrete standards for its implementation must be assessed on the basis of reasonableness and developments in State practice.

3.5.3. Obligations of the Third State

Digital communications are almost always cross-border. A message sent from an embassy to the foreign ministry of the sending State may pass through undersea cables, internet exchange points, data centers, and other infrastructure in several jurisdictions.

This characteristic makes Article 40(3) of the VCDR increasingly important. That provision requires third States to accord official communications in transit the same freedom and protection as is accorded by the receiving State.

Historically, the provision was drafted when diplomatic transit was more easily identified through the movement of couriers and messages. In the digital environment, patterns of transit are far more complex. Nevertheless, the underlying principle remains relevant: the legal status of diplomatic communications should not be lost merely because the communications technically pass through a third jurisdiction.

This also reveals one of the greatest problems of contemporary diplomatic communication: the mismatch between legal protection, which follows the function of communication, and internet architecture, which follows the location of infrastructure.

3.5.4. Obligations of the Sending State

The protection of diplomatic communications is not an unlimited right. Article 41 of the VCDR still requires the sending State and members of the mission to respect the laws of the receiving State and not to use diplomatic premises in a manner inconsistent with the functions of the mission.

If diplomatic channels or mission facilities are used to carry out intelligence operations incompatible with diplomatic functions, the receiving State retains the legal means available within the diplomatic regime. It may request the recall of the officials concerned, declare a person *persona non grata*, or take other diplomatic measures permitted by the VCDR.

However, alleged abuse does not in itself extinguish the inviolability of communications. The principle that can be drawn from *Tehran Hostages* is that an alleged violation by one party does not entitle the other party to disregard the fundamental obligations of diplomatic law.

The second finding of this study is therefore that the protection of Article 27 is layered: the receiving State bears negative and positive obligations, third States bear obligations with respect to communications in transit, and the sending State remains bound by the prohibition on abusing diplomatic facilities.

3.6. State Practice and the Significance of Indonesia's Response

The surveillance of Indonesian officials revealed in 2013 illustrates the political consequences of the interception of inter-State communications. Indonesia responded to the disclosure by recalling its ambassador from Canberra for consultations, requesting an explanation, and evaluating certain relations and cooperation.

This case cannot be treated as a direct example of a violation of Article 27, because the communications targeted were primarily those of senior State officials rather than clearly the official correspondence of a diplomatic mission. Nevertheless, it remains relevant as evidence of State reactions to surveillance practices.

Indonesia's diplomatic reaction shows that interception was not passively accepted as a normal practice of international relations. This matters because State practice that is conducted in secret, denied, or consistently protested by other States is difficult to rely on for an argument that general acceptance of the interception of diplomatic communications has formed.

The alleged wiretapping of the Embassy of the Republic of Indonesia (KBRI) in Yangon is one example of a problem concerning the protection of diplomatic communications discussed in Indonesian legal literature. Mangku (2010) examines the allegation under the 1961 VCDR and emphasizes the importance of the principle of inviolability for diplomatic representations. However, the information on the event in this study still rests on secondary studies and is not supported by official investigative documents or legal decisions confirming that a violation occurred. The Yangon case is therefore treated as an allegation of normative relevance, not as an established fact of a violation of Article 27 of the VCDR. This distinction is important to ensure that the legal analysis does not equate media reports or alleged intelligence activity with proof of State responsibility under international law.

Other State practice shows that surveillance of diplomatic communications and of the communications of State officials has prompted various official responses. In

2013, the Government of Ecuador announced the discovery of a listening device in the Ecuadorian Embassy in London and requested the cooperation of the United Kingdom Government in investigating those responsible (Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, 2013). Around the same time, the German Government asked the United States for clarification after information emerged about the possible monitoring of Chancellor Angela Merkel's telephone and stated that such a practice would be unacceptable if proven true (Federal Foreign Office, 2013b). Brazil and Germany subsequently introduced a joint initiative on the privacy of digital communications at the United Nations (Federal Foreign Office, 2013a). Although the Ecuadorian case relates more directly to the security of a diplomatic representation, whereas the German and Brazilian cases concern chiefly the surveillance of State officials' communications and the right to privacy, all three show State responses to alleged or suspected cross-border interception of communications.

A multilateral response can be seen in United Nations General Assembly Resolution 68/167 of 2013 on *The Right to Privacy in the Digital Age*, which highlights the risks that electronic surveillance, interception of digital communications, and data collection pose to the realization of the right to privacy (United Nations General Assembly, 2013). In addition, the 2015 report of the United Nations Group of Governmental Experts (UN GGE) and the 2021 report of the Open-ended Working Group (OEWG) affirm the applicability of international law to States' use of information and communications technologies (United Nations General Assembly, 2015, 2021). These diplomatic practices and multilateral documents indicate State attention to the protection of digital communications, but they are not sufficient to prove the formation of a general practice accepted as law (*opinio juris*) concerning a specific prohibition on the interception of diplomatic communications under Article 27 of the VCDR. Assessing general practice and *opinio juris* requires evidence of the consistency of State conduct and of a belief that such conduct is undertaken under a legal obligation. Accordingly, in this study, developments in State practice and United Nations responses are treated as supporting material for interpretation, not as conclusive evidence of the formation of a new customary norm on the cyber interception of diplomatic communications.

Timor-Leste v. Australia offers an additional perspective. The case was not decided under Article 27 of the VCDR, but the Court's order on provisional measures demonstrates the importance of protecting the confidentiality of a State's documents and communications. It shows that the confidentiality of State data may constitute a legal interest serious enough to warrant interim protection in international judicial proceedings.

Accordingly, the practice of Indonesia, Ecuador, Germany, and Brazil, together with the multilateral responses through the United Nations, shows a growing concern for protecting communications against surveillance and interception. However, the variation in the objects of protection, legal bases, and forms of State response does not yet permit the conclusion that a general practice and *opinio juris* have formed that

specifically prohibit the cyber interception of diplomatic communications under Article 27 of the VCDR. If anything, this finding reinforces the need for a systematic interpretation of the diplomatic law provisions already in force.

3.7. Reinterpreting Article 27 of the VCDR for the Cyber Era

On the basis of the analysis as a whole, this study yields four principles for reinterpreting Article 27 of the VCDR that can be used to understand the protection of diplomatic communications in the digital environment.

3.7.1. *The Principle of Medium Neutrality*

Protection must be determined by the communication's relationship to the diplomatic function, not by the technology used. E-mail, communications over private networks, internet-based calls, and encrypted instant messages may all constitute official correspondence when used in carrying out the mission's functions.

This principle derives from the functional definition in Article 27(2) and the open-ended character of the phrase *all appropriate means* in paragraph 1. Accordingly, technological change does not alter the legal nature of the communication.

3.7.2. *The Principle of Location Independence*

The protection of official communications does not end when data leave the embassy premises. Article 24, on archives and documents "wherever they may be," and Article 40(3), on communications in transit, provide a systematic basis for the proposition that diplomatic protection does not always depend on the physical location of the information.

This principle is especially important for the use of cloud computing systems and cross-border infrastructure.

3.7.3. *The Principle of Layered Obligations*

The protection of diplomatic communications comprises several levels of obligation. The receiving State has a negative obligation not to intercept and a positive obligation to take reasonable protective measures. Third States have obligations with respect to official communications in transit, while the sending State must prevent the abuse of diplomatic facilities.

This structure shows that the security of diplomatic communications is a normative responsibility distributed among several State actors.

3.7.4. *The Principle of Confidentiality and Availability*

Article 27 protects not only the content of communications from unauthorized access. The phrase "free communication" also requires that a mission be able to send and receive communications effectively.

Accordingly, cyber operations that do not read content but block, disrupt, or render communication channels unavailable may still contravene Article 27(1). *Denial-of-service* attacks, channel disruption, or other acts that significantly impede official communications can be analyzed under the obligation to permit free communication.

The right to use code and cipher also shows that the protection of confidentiality is indeed part of the design of Article 27. In the modern context, the use of encryption is the functional equivalent of the right to use code or cipher that the VCDR has recognized from the outset.

These four principles are the principal findings of this study. This model distinguishes the study from approaches that attempt to create new categories within diplomatic law. The proposed reinterpretation continues to operate within the structure of the VCDR by extending the application of generic terms on the basis of function and technological development.

3.8. Implications of the Reinterpretation for Indonesia

The reinterpretation of Article 27 has two implications for Indonesia, because Indonesia is both a receiving State for foreign diplomatic representations and a sending State with representations in many countries.

The reinterpretation of Article 27 of the VCDR carries implications for Indonesia as both a receiving and a sending State of diplomatic missions. Law No. 1 of 1982 and Law No. 37 of 1999 provide the basis for diplomatic protection, whereas the wiretapping powers under Law No. 17 of 2011 on State Intelligence and the Electronic Information and Transactions Law, as well as the data-protection exceptions in Law No. 27 of 2022, may give rise to problems if applied to a diplomatic mission's official communications. Harmonization of the application of national regulations and inter-agency guidelines is therefore needed so that State powers continue to respect the principle of inviolability under Article 27 of the VCDR.

As a receiving State, Indonesia is obliged to ensure that its domestic legal framework does not generate acts contrary to the inviolability of diplomatic communications. Indonesia has ratified the VCDR through Law No. 1 of 1982 and treats international diplomatic law as an important component of the conduct of foreign relations.

In the digital environment, harmonization is needed between that obligation and the national regimes on wiretapping, personal data protection, cybersecurity, telecommunications, and access to electronic systems. National provisions that confer powers of access or interception must be applied with due regard for the special protection attaching to diplomatic communications.

This need is all the more pressing because diplomatic communications may use the infrastructure of private electronic system operators. More explicit national guidelines could reduce uncertainty about how officials, regulators, and service providers should treat data that is legally the official communication of a diplomatic mission.

As a sending State, Indonesia likewise cannot rely solely on the legal protection afforded by the receiving State. The communications architecture of Indonesia's representations needs to be built on a defense-in-depth approach. This may include

encryption standards, key management, communication classification, segmentation between official and personal communications, device management, incident-response procedures, and the documentation of technical evidence.

Technical documentation has legal relevance because one of the greatest obstacles in cyber disputes is attribution. A State cannot effectively bring a legal claim or protest if it lacks adequate information about the source, methods, and effects of an operation.

At the level of foreign policy, Indonesia also has an interest in clarifying its national position on the application of international law in cyberspace. A statement that Article 27 of the VCDR covers electronic communications could offer two benefits. First, it would clarify Indonesia's obligations toward foreign representations. Second, it would strengthen Indonesia's position when the communications of its representations abroad are intercepted or disrupted.

Such a statement could also contribute to the formation of State practice. The more States express consistent interpretations of the protection of digital diplomatic communications, the stronger the basis for identifying a shared understanding of how the VCDR applies to new technologies.

4. CONCLUSION

This study concludes, first, that Article 27(1) and (2) of the 1961 VCDR can be applied to electronic diplomatic communications through evolutive interpretation under Articles 31 and 32 of the 1969 VCLT. Second, the cyber interception of a diplomatic mission's official communications should be analyzed through diplomatic law as *lex specialis*, which places obligations of protection on the receiving State and third States in accordance with the VCDR. Third, the reinterpretation of Article 27 yields four principles: medium neutrality, location independence, layered obligations, and the protection of the confidentiality and availability of communications.

For Indonesia, guidelines on the protection of digital diplomatic communications need to be prepared through coordination among the Ministry of Foreign Affairs, intelligence agencies, and law-enforcement authorities, including the harmonization of wiretapping powers with the principle of diplomatic *inviolability*. Future research is encouraged to examine State practice comparatively, the status of metadata protection, and the standards of *due diligence* and of proof of attribution in cyber interception.

REFERENCES

- ABC News. (2013). *Indonesia recalls ambassador after leaked documents reveal Australia spied on President Susilo Bambang Yudhoyono*. <https://www.abc.net.au/news/2013-11-18/indonesia-angered-by-revelations-australia-spied-on-sby/5100264>

- Al Jazeera. (2013a). *Indonesia recalls envoy over Australia spying*.
<https://www.aljazeera.com/news/2013/11/18/indonesia-recalls-envoy-over-australia-spying>
- Al Jazeera. (2013b). *Spying rocks Indonesia-Australia relations*.
<https://www.aljazeera.com/features/2013/11/22/spying-rocks-indonesia-australia-relations>
- Anstis, S. (2024). Regulating transnational dissident cyber espionage. *International & Comparative Law Quarterly*, 73(1), 259–274.
<https://doi.org/10.1017/S0020589323000532>
- Arato, J. (2010). Subsequent practice and evolutive interpretation: Techniques of treaty interpretation over time and their diverse consequences. *The Law & Practice of International Courts and Tribunals*, 9(3), 443–494.
<https://doi.org/10.1163/157180310X539511>
- Biglarbeigi, K., & Azizi, S. (2026). The interaction of diplomatic and consular law with cyber operations in light of the Tallinn Manual 2.0. *Public Law Research*, 28(91), 227–284. <https://doi.org/10.22054/qjpl.2025.83725.3067>
- Broeders, D. (2024). Cyber intelligence and international security: Breaking the legal and diplomatic silence? *Intelligence and National Security*, 39(7), 1213–1229.
<https://doi.org/10.1080/02684527.2024.2398077>
- Butt, S. (2014). The position of international law within the Indonesian legal system. *Emory International Law Review*, 28(1). <https://law.emory.edu/eilr/content/volume-28/issue-1/recent-developments/international-law-indonesian-legal-system.html>
- Chircop, L. (2019). Territorial sovereignty in cyberspace after Tallinn Manual 2.0. *Melbourne Journal of International Law*, 20(2).
<https://law.unimelb.edu.au/mjil/issues/issue-archive/volume-202-december-2019>
- Denza, E. (2025). *Diplomatic law: Commentary on the Vienna Convention on Diplomatic Relations* (5th ed.). Oxford University Press.
<https://doi.org/10.1093/law/9780198974857.001.0001>
- Federal Foreign Office. (2013a). *Foreign Minister Westerwelle on the UN resolution “The right to privacy in the digital age.”* <https://www.auswaertiges-amt.de/en/newsroom/news/131101-brasilien-vn-258082>
- Federal Foreign Office. (2013b). *Statement regarding information that the Federal Chancellor’s cellphone may have been monitored by US intelligence services*.
<https://www.auswaertiges-amt.de/en/newsroom/news/131024-sts-seibert-ueberwachung-merkel-257954>
- Hoang, L. (2013). *Indonesia, Australia mend ties after surveillance scandal*.
<https://www.globalsecurity.org/military/library/news/2013/12/mil-131205-voa07.htm>
- International Court of Justice. (2009). *Dispute regarding navigational and related rights (Costa Rica v. Nicaragua): Judgment of 13 July 2009*.

- International Court of Justice. (2014). *Questions relating to the seizure and detention of certain documents and data (Timor-Leste v. Australia): Order on provisional measures of 3 March 2014*.
- International Court of Justice. (2015). *Questions relating to the seizure and detention of certain documents and data (Timor-Leste v. Australia): Order of 22 April 2015 on the request for modification of provisional measures*.
- International Law Commission. (1958). Draft articles on diplomatic intercourse and immunities with commentaries. In *Yearbook of the International Law Commission* (Vol. 1958). United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_1_1958.pdf
- Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and insights. *Georgetown Journal of International Law*, 48(3). <https://www.law.georgetown.edu/international-law-journal/in-print/volume-48/volume-48-number-3-spring-2017/the-tallinn-manual-2-0-highlights-and-insights/>
- Kenny, J. (2024). Cyber operations and the status of due diligence obligations in international law. *International & Comparative Law Quarterly*, 73(1), 135–176. <https://doi.org/10.1017/S0020589323000489>
- Mačák, K. (2025). A missed opportunity: An international law perspective on the final OEWG report. *EJIL: Talk!* <https://www.ejiltalk.org/a-missed-opportunity-an-international-law-perspective-on-the-final-oweg-report/>
- Mangku, D. G. S. (2010). Violation of diplomatic immunity rights (A case study of the wiretapping of the Embassy of the Republic of Indonesia (KBRI) in Yangon, Myanmar, under the 1961 Vienna Convention). *PERSPEKTIF: Kajian Masalah Hukum dan Pembangunan*, 15(3), 226–261. <https://doi.org/10.30742/perspektif.v15i3.54>
- Max Planck Encyclopedia of Public International Law. (n.d.). *Vienna Convention on Diplomatic Relations (1961)*. Oxford University Press. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1004>
- Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador. (2013). Ecuador launches investigation to determine who planted a spy microphone in Ecuador's Embassy in London. <https://www.cancilleria.gob.ec/2013/07/03/ecuador-inicia-investigaciones-para-determinar-quien-coloco-un-microfono-espia-en-la-embajada-de-ecuador-en-londres/>
- Moulin, T. (2026). The law of diplomatic relations. In *Cyber-espionage in international law: Silence speaks* (pp. 182–201). Manchester University Press.
- NATO Cooperative Cyber Defence Centre of Excellence. (2025). *Handbook on developing a national position on international law and cyber activities: A practical guide for States*. https://ccdcoe.org/uploads/2025/05/Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf

- Roberts, I. (2023). Diplomatic communication. In *Satow's diplomatic practice* (8th ed., pp. 115–126). Oxford University Press.
<https://doi.org/10.1093/law/9780192859594.003.0007>
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.
https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf
- United Nations. (1961). *Vienna Convention on Diplomatic Relations*. United Nations.
- United Nations General Assembly. (2013). *The right to privacy in the digital age*. United Nations. <https://digitallibrary.un.org/record/764407>
- United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations.
https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf
- United Nations General Assembly. (2021). *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final substantive report*. United Nations.
<https://documents.un.org/doc/undoc/gen/n21/068/72/pdf/n2106872.pdf>
- Zhahira, T. N., & Christianti, D. W. (2023). The establishment of a virtual embassy according to the 1961 Vienna Convention on Diplomatic Relations: The case of Barbados' metaverse embassy. *Jurnal Bina Mulia Hukum*, 8(1), 106–127.
<https://doi.org/10.23920/jbmh.v8i1.1336>



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).
