

ROMANIAN JOURNAL OF INTERNATIONAL LAW

ISSN 2559 – 3846

Reinterpreting the Diplomatic Inviolabilities in the Vienna Convention on Diplomatic Relations in the Era of New Technologies

Ioana-Alexandra SMĂRĂNDESCU

RJIL No. 33/2025

Pages 79-96

Reinterpreting the Diplomatic Inviolabilities in the Vienna Convention on Diplomatic Relations in the Era of New Technologies*

*Ioana-Alexandra SMĂRĂNDESCU***

University of Bucharest

Abstract: *This article examines the challenges regarding the diplomatic inviolabilities contained in the Vienna Convention on Diplomatic Relations (1961) in the current high-tech era. As new technologies begin to reshape international relations, the diplomatic activity must adapt to new challenges. In recent years, there have been numerous incidents targeting diplomatic activity. Little by little, the Vienna Convention, the cornerstone of diplomatic law, is no longer capable of insuring the protection of this activity. Despite the efforts of scholars, notably the experts involved in the creation of the Tallinn Manual 2.0, “modern” diplomatic inviolabilities remain an unregulated branch of international law. This study aims to highlight the need for a stronger response from the international community regarding this aspect. By addressing this issue, this article contributes to the ongoing discussions regarding the adaptation of traditional institutions of international law to cyberspace and its specificities.*

Keywords: *diplomatic inviolabilities, cyberspace, electronic archives, cyber diplomacy.*

* *The present article represents an adaptation of the author's LL.M. dissertation, titled “Reinterpreting the diplomatic inviolabilities in the Vienna Convention on Diplomatic Relations in the era of new technologies” which was presented in July 2025, at the Faculty of Law at the University of Bucharest.*

** *Ioana Smarandescu is a diplomat at the Ministry of Foreign Affairs of Romania. She is also a graduate of University of Bucharest Faculty of Law (Bachelor of Laws and LL.M.s in Public International Law and New Technologies Law) and of University Paris I Pantheon Sorbonne’s Collège franco-roumain d’études européennes (Bachelor of Laws).*

The opinions expressed in this paper are solely the author’s and do not engage the institutions she belongs to.

Introduction

International relations are increasingly influenced by emerging technologies. The development of cyberspace and the progressive use of Artificial Intelligence in warfare are just some of the subjects that captivated the general public in the last years. In such an effervescent world, the diplomatic activity finds itself exposed to new and complex threats¹.

In recent years, numerous incidents related to cyber operations have highlighted how vulnerable diplomats truly are. It was suggested that the Vienna Convention, once the bedrock of diplomatic law, is struggling to provide protection in today's digital environment².

Despite recent contributions of legal scholars, the concept of "modern" diplomatic inviolability remains largely unaddressed in international law. This article aims to highlight the need for an "updated" response from the international community regarding this issue.

Diplomatic inviolability refers to the principle that diplomatic agents, the premises where they conduct their activity and their means of accomplishing their missions are protected from interferences of host States. This concept is central to the stability of international relations.

Caught in the middle of a rapidly changing world, one cannot help but wonder: can the institution of diplomatic inviolability survive in the digital era without fundamentally rethinking the current international legal norms of the Vienna Convention on Diplomatic Relations? In the following pages, the author will try to analyze this issue.

1. Traditional Diplomatic Law

Diplomatic law represents the "field of international law concerning the practice of diplomacy and the rights and obligations of state representatives on the territory of other States"³. At the core of diplomatic law stands the

¹ Lazăr Elena, *Jurisdiction et cybercriminalité*, Revue TIC, Innovation et droit international, Ed. Pedone, 2017

² Jovan Kurbalija, *Is it time for a review of the Vienna Convention on Diplomatic Relations?*, 16th april 2012, www.diplomacy.edu/blog/it-time-review-vienna-convention-diplomatic-relations/, read on 10th January 2025.

³ *Diplomatic Law* (LII / Legal Information Institute), www.law.cornell.edu/wex/diplomatic_law, read on 10th January 2025.

institution of diplomatic inviolability.⁴ In Ancient Greece and in the Roman Empire, envoys enjoyed protection and were considered essential for maintaining good relations with other States⁵. Messengers were crucial for harmony between kingdoms⁶ and, consequently, enjoyed special treatment, as a form of respect towards the sending State itself.

With the Treaty of Westphalia (1648), the concept of *State* was established. States were recognized as sovereign, independent in relation to other States and enjoying supremacy on the national scene. Rulers agreed to respect internationally-recognized borders and to treat other States as equal subject on the international scene. Subsequently, the representatives of these States were also granted a special form of recognition, in respect for the functions they had to accomplish.

By the end of the seventeenth century, there was already a well-established practice of granting immunity to representatives of States⁷, rules that can be considered the foundation of diplomatic law today. For example, in 1758, Vattel, in his work *Le Droit des gens*, was already offering clear overview of the existent rules of diplomatic immunity at the time⁸. State practice remained constant for the next two hundred years⁹. In 1815, after the downfall of Napoleon Bonaparte, at the Congress of Vienna, the first international instrument to codify aspects of diplomatic law was adopted¹⁰. These rules

⁴ On the related issue of immunity of state officials and its interactions with other obligations, such as the obligations to extradite and prosecute, see Filip Andrei Lariu, Immunity as a Circumstance Excluding the Operation of the Obligation to Extradite or Prosecute – Part I: The Principle of *aut Dedere aut Judicare*”, RJIL, 27/2022, “Part II: Immunities and the Existence of a Conflict of Norms”, RJIL, No. 28/2022 and “Part III: The Effects of Immunities on the Obligation to Extradite or Prosecute”, RJIL, No. 29/2023.

⁵ Felipe López-Valencia, *Diplomatic Shield: The Historical Origin and Dynamics of Diplomatic Immunity in Public International Law*, 4th October 2023, dip.uexternado.edu.co/uncategorized/diplomatic-shield-the-historical-origin-and-dynamics-of-diplomatic-immunity-in-public-international-law .

⁶ K.A.A.N. Thilakarathna Akalanka, *The Evolution Of The Vienna Convention On Diplomatic Relations And Consular*, www.academia.edu/The_Evolution_Of_The_Vienna_Convention_On_Diplomatic_Relations_And_Consular.

⁷ Eileen Denza, *Commentary on the Vienna Convention Diplomatic Relations. A commentary* (2016), Oxford University Press, p. 1.

⁸ *Ibidem*.

⁹ Commentary on Vienna Convention (n 1).

¹⁰ *Vienna Convention on Diplomatic Relations* United Nations, Audiovisual Library of International Law, 18 April 1961, legal.un.org/avl/ha/vcdr/vcdr.html.

regarded the classes of heads of diplomatic missions and their order of precedence. Finally, in 1961, the customary law was finally comprised in one treaty, the Vienna Convention on Diplomatic Relations. Two years later, the Vienna Convention on Consular Relation followed.

The Vienna Convention on Diplomatic Relations is considered to be one of the most successful treaties ever created¹¹. The International Court of Justice (ICJ), the main judicial organ of the United Nations, ruled that this Convention enjoys so much success because it is “accepted through the world by nations of all creeds, cultures and political complexions”.¹² Its importance cannot be denied. In the following pages, the author will make a brief analysis of the articles regarding diplomatic inviolability, which stand at the heart of the Convention.

1.1. Inviolability of the Diplomatic Missions

Article 22, paragraph 1 of the Vienna Convention refers to the premises of the mission, the *physical* space where most of the diplomatic activities are being exercised. At first glance, it may seem that the provision only protects the actual building of the diplomatic mission. However, the term *premises* has a broader sense. It refers to buildings, parts of buildings, pieces of land that are necessary for the activity of the mission and the official residence of the Head of mission.¹³ These entities constitute *premises* in the sense of the Convention irrespective of their ownership.¹⁴ They could belong to the sending State, to the receiving State or can simply be rented from privates, for the exercise of diplomatic purposes. What matters is the diplomatic activity conducted within, which will determine their special status in international law.

The premises of the mission are protected from any law-enforcement operation conducted by the authorities of the receiving State that can hinder the activity of the mission.¹⁵ Exceptionally, the receiving State’s authorities can enter the premises if the Head of Mission allows it. Some scholars have

¹¹ Behrens P, *Diplomatic Law in a New Millennium, In the praise of a self-contained regime. Why the Vienna Convention on Diplomatic Relations remains important today*, Oxford University Press 2017, p. 23.

¹² Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran); [1981] ICJ, Order, 12 V 81.

¹³ Vienna Convention (n 2).

¹⁴ Vienna Convention (n 3).

¹⁵ Vienna Convention (n 4).

even suggested that private individuals are under the same obligation to refrain from hindering the activity of the mission.¹⁶

Article 22 was envisaged to cover objects that have a physical existence: buildings, pieces of land, residences of the members of the diplomatic corps. For *traditional* diplomatic law, sovereignty and jurisdiction maintain a strict link to territoriality.¹⁷ One can easily observe that the provisions of the Vienna Convention were imagined in a world that was still “Westphalian”. However, with the development of the new technologies, territoriality begins to lose its importance. In fact, the majority of the diplomatic activity can be conducted from afar, without the necessity of physically being on the territory of one’s State. After the COVID 19 pandemic, for example, the number of virtual videoconferences has increased, limiting the number of face-to-face meetings between diplomats. Naturally, this phenomenon had an important influence on the diplomatic activity.

1.2. Inviolability of Archives and Documents

Article 24 stipulates that “the archives and documents of the mission shall be inviolable at any time and wherever they may be”¹⁸. But what exactly constitutes a *document* or a diplomatic *archive*? The preparatory work of the Convention confirms that the term must be broadly interpreted.¹⁹ The provision was never intended to solely cover physical documents (confidential papers, notes from ambassadors, orders from the central administration of the sending State etc.) that can be found within the premises of the diplomatic mission. That is why there is no exhaustive list provided by the Convention. However, the Vienna Convention on Consular Relations does offer such a list for the term *consular archive*: “all the papers, documents, correspondence, books, films, tapes and registers of the consular post, together with the ciphers and codes, the card-indexes and any article of furniture intended for their protection or safekeeping”.²⁰ In practice, this definition has been applied by analogy to diplomatic relations²¹. The reason behind this practice is that diplomatic relations are much more extended than consular ones, so the term *archives* should also be interpreted at least to this

¹⁶ Paul Behrens, *Diplomatic law in a new millennium...*, p. 173.

¹⁷ Ibidem.

¹⁸ Article 24 of the Vienna Convention on Diplomatic Relations.

¹⁹ Eileen Denza (n 4).

²⁰ Vienna Convention on Consular Relations, article 1(1)(k).

²¹ Eileen Denza (n 5).

extent.²² Foreign policy objectives cannot be fulfilled without diplomatic activity, which encompasses a wide range of actions. While safeguarding national interest, State's representatives must also find ways to promote mutual interests. This aim requires coordinated responses and strategies, which require more action than in the case of consular relations.

Article 24 permits a wide interpretation and it is perfectly adaptable to today's new forms of communications. In the light of this provision, new types of *documents* and *archives* could benefit from protection. Some aspects are particularly interesting in this regard. Virtual embassies, social media platforms of the missions, smartphone apps, digital task forces, big data used for diplomatic purposes²³ could fall under this provision, therefore being inviolable.

1.3. Inviolability of the Diplomatic Personnel

Article 29 of the Vienna Convention on Diplomatic Relations stipulates that “the person of a diplomatic agent shall be inviolable. He shall not be liable to any form of arrest or detention. The receiving State shall treat him with due respect and shall take all appropriate steps to prevent any attack on his person, freedom or dignity.²⁴” This rule is the oldest rule in diplomatic law²⁵.

When interpreting article 29, the inviolability of the diplomatic personnel is understood as an interdiction to charge, arrest the diplomat or search through his/her personal belongings.²⁶ In the light of new technologies, there are new actions that may violate this provision. Surveillance of the activity of diplomats or data theft can be covered by this provision. Considering how diplomacy evolved over the years from its traditional form to a more “visible” diplomacy²⁷, in which the diplomat addresses not only States, but also individuals and other multiple stakeholders, these concerns are becoming more and more acute for the diplomatic corps around the world.²⁸ Visibility brings the diplomat closer to its goals, but sometimes visibility can also mean vulnerability. Cyberspace is the perfect example.

²² Ibidem.

²³ Corneliu Bjola, Ilan Manor, *The rise of hybrid diplomacy: from digital adaptation to digital adoption*, *International Affairs* 98: 2, 2022, p. 2.

²⁴ Article 29 of the Vienna Convention on Diplomatic Relations.

²⁵ Eileen Denza (n 6).

²⁶ Vienna Convention on Diplomatic Relations.

²⁷ Paul Behrens, *Diplomatic law in a new millennium...*, p. 33.

²⁸ Ibidem.

After briefly presenting the main provisions of the Vienna Convention, we will now analyze the new challenges regarding diplomatic inviolabilities.

2. Diplomatic Law and the Challenges of New Technologies

In the context of the evolution of cyber warfare techniques, scholars have started to envisage how certain branches of international law may be adapted to cyberspace. NATO's Cooperative Cyber Defence Centre of Excellence has created the Tallinn Manual, an outstanding initiative that aims to clarify numerous "cyber issues". In the following pages, the author will focus on the second version of the manual, in order to analyze the latest developments of diplomatic inviolabilities.

2.1. Establishing New Conditions for the Diplomatic Mission's Inviolability

Rule 39 of the Tallinn Manual stipulates the inviolability of the diplomatic premises in which cyber infrastructure is located²⁹. Starting from the definition of the term "premises" contained in article 1, letter (i) of the Vienna Convention³⁰, the experts have added a new condition regarding the protection of diplomatic missions in the context of cyber operations: that the critical infrastructure must be located *inside* the premises of the mission.³¹ *A contrario*, a cyber infrastructure that can be found outside of the premises does not benefit from the inviolability of the mission. Moreover, only the critical infrastructure that is used for the activity of the mission is being protected under this provision³².

It is interesting that the experts have decided to link the application of the inviolability rule to the actual location of the infrastructure. By imposing this condition, they have limited the scope of the provision.

Scholars have wondered if portable objects, used in the diplomatic activity, outside of the premises of the diplomatic mission, could be protected by the

²⁹ Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press 2018, rule 39.

³⁰ Article 1, letter (i) of the Vienna Convention on Diplomatic Relations stipulates that the "premises" are the buildings, parts of buildings and land ancillary used for the purpose of the mission, including the residence of the head the mission.

³¹ Tallinn Manual 2.0 (n 1).

³² Tallinn Manual 2.0 (n 3).

inviolability of the diplomatic mission³³. Article 22, paragraph 3 of the Vienna Convention on Diplomatic Relations stipulates that: “The premises of the mission, their furnishing and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution.”³⁴ Gadgets such as phones, laptops or other portable devices could be connected to the ICT infrastructure of the Ministry of Foreign Affairs (MFA). Because of the fact that the diplomat can access sensitive information by using these devices, some scholars have asked themselves if these objects should also enjoy inviolability, as movable goods “linked” to the premises³⁵.

The opinions of the experts varied. Some scholars believed that inviolability extends to these gadgets as well. They claimed that a different interpretation contravenes the main goal of the provision.³⁶ Therefore, any cyber operation conducted against these objects outside of the diplomatic premises would violate the rule³⁷. This interpretation was also upheld by the systemic interpretation that the Vienna Convention on Diplomatic Relations provides that the movable property of diplomats remains inviolable. Other experts were more reticent to this interpretation. They emphasized that these movable goods are only immune to search, requisition, attachment, execution³⁸. Therefore, when it comes to cyber operations, they should only be protected in the exceptional cases mentioned above³⁹. A few experts argued that this type of property should enjoy no protection whatsoever⁴⁰.

Rule 40 of the Tallinn manual, named *Duty to protect cyber infrastructure*, stipulates that “A receiving State must take all appropriate steps to protect cyber infrastructure on the premises of a sending State’s diplomatic mission or consular post against intrusion or damage”⁴¹. Once again, the emphasis is put on the physical presence of cyber infrastructure on the premises of the diplomatic mission or the consular post. Therefore, the receiving State’s main

³³ Tallinn Manual 2.0 (n 4).

³⁴ Vienna Convention on Diplomatic Relations, article 22, paragraph 3.

³⁵ Ibidem.

³⁶ Tallinn Manual 2.0 (n 5).

³⁷ Ibidem.

³⁸ Tallinn Manual 2.0 (n 6).

³⁹ Tallinn Manual 2.0 (n 7).

⁴⁰ Tallinn Manual 2.0 (n 8).

⁴¹ Tallin Manual 2.0 (n 10).

obligation is to make sure that this infrastructure is not harmed, in any way, by any type of unwanted activity. This is a *special duty* of the receiving State, one specific to cyberspace. Apart from ensuring the protection of the premises of the mission itself, States must now protect a specific immobile good within the premises of the mission, which is the cyber infrastructure. The experts have highlighted the fact that, the moment the authorities of the receiving State (the legal subject that holds this obligation) are aware of the fact that the infrastructure of the mission is being targeted by malicious activity, they have the obligation to protect it.⁴² The obligation is not one of result, as the receiving State must *engage in all reasonable effort* to terminate the malicious attack against the mission⁴³. Therefore, the obligation is one of best efforts. If the situation demands it, the receiving State even has the obligation to notify the authorities of the sending State to inform them about the threat and the steps that need to be taken further⁴⁴.

In order to be able to effectively tell if the receiving State fulfilled this obligation, some conditions may be considered. Tallinn Manual 2.0 mentions the *magnitude of the threat posed to the premises, the extent to which the receiving State was aware of the threat* and, last but not least, *the capabilities of the receiving State* (including its own cyber infrastructure) to detect such threats.⁴⁵ As it can be observed, this is a case-by-case analysis in order to assess whether or not the receiving State respected its obligations. What is certain is that the standard for States that have a well-established cyber infrastructure will be different from those that are less experienced regarding cyberspace. The former will have to be very convincing in demonstrating why they did not react to the threat or why they took a specific measure, whereas for the latter the standard of proof will be less restrictive. Unfortunately, this may raise numerous difficulties in practice. A case-by-case analysis must be conducted regarding every specific incident.

Because of the difference in States' technological development, some scholars wondered if a receiving State can demand the assistance of other States, third-parties, in order to effectively defend the cyber infrastructure within a diplomatic mission.⁴⁶ Once again, there was no consensus on the matter. The term *appropriate steps* does not imply, for the majority of the

⁴² Tallinn Manual 2.0 (n 11).

⁴³ Tallinn Manual 2.0 (n 12).

⁴⁴ Tallinn Manual 2.0 (n 13).

⁴⁵ Tallinn Manual 2.0 (n 14).

⁴⁶ Ibid.

experts, that a receiving State must request help from another State. Therefore, the rule limits the action of the State to what it alone can do⁴⁷. Other experts believed the contrary. As the obligation is one of best efforts, one State can seek assistance from States that have a more developed cyber infrastructure⁴⁸.

When it comes to preventive actions, the experts concluded that the receiving State has no obligation to take preventive measures to protect the premises of the diplomatic mission.⁴⁹ This opinion was supported by State practice.⁵⁰ In traditional diplomatic law, the receiving State is under no obligation to offer protection to the premises in the absence of an imminent risk.⁵¹ Only if there is a real, quantifiable risk regarding the premises, there is an obligation to take action.⁵²

The receiving State is, however, under the obligation to make sure that the activity of the mission is not, in any way, hindered.⁵³ It is unclear how far the receiving State should go in order to comply with this provision. If social media users write threatening comments on the Facebook page of a foreign embassy, it was concluded that this act, in itself, does not necessitate an answer from the receiving State, as it cannot constitute a serious disturbance of the mission's activity.⁵⁴ Therefore, a higher level of disturbance must be attained in order to apply this provision. If, in traditional diplomatic law, attacks on embassies, protests and attempts to trespass their perimeter constitute acts that demand an according response from the receiving State, in cyberspace, DDoS, ransoms or attacks that disturb the activity of embassies may be actions that demand a strong and equally-proportionate response from the receiving State's authorities. This is a case-by-case analysis to conclude that the degree is high enough to necessitate action.

There have been numerous attacks against embassies in recent years. Some perpetrators have specialized themselves into exploiting the vulnerabilities of the diplomatic activity conducted in cyberspace. The Golden Jackal is one

⁴⁷ Tallinn Manual 2.0 (n 15).

⁴⁸ Tallinn Manual 2.0 (n 16).

⁴⁹ Tallinn Manual 2.0 (n 17).

⁵⁰ Tallin Manual 2.0 (n 18).

⁵¹ Tallin Manual 2.0 (n 19).

⁵² Tallin Manual 2.0 (n 20).

⁵³ Tallinn Manual 2.0 (n 21).

⁵⁴ Tallinn Manual 2.0 (n 23).

threat actor known for its attacks against embassies and governmental organizations. Its goal is to steal confidential data from high-profile systems.⁵⁵ They do not target systems that are connected to the internet.⁵⁶ Reports show that there were three main types of malware used in the case of the South Asian embassy attacked: the GoldenDealer, GoldenHowl and GoldenRobo⁵⁷. GoldenDealer consisted of executables that were introduced in the systems via compromised USB drives⁵⁸. GoldenHowl was creating a modular backdoor, which helped stealing files, creating tasks and SSH tunneling.⁵⁹ GoldenRobo was the exfiltration tool.⁶⁰ Moreover, two more types of malware, the GoldenMailer and GoldenDrive, were used to steal data via email and Google Drive⁶¹.

Another example occurred in 2024 and it involved Russian-sponsored actors who were targeting French diplomatic entities. The hostile actions were disclosed by the ANSSI (Autorité nationale de la sécurité des systèmes d'information), the French Cybersecurity Agency. The culprit was the group known as Midnight Blizzard.⁶² ANSSI has shown in its report that numerous diplomatic entities were targeted, from embassies of Western countries to Ministries of Foreign Affairs⁶³, alongside public institutions, such as the French Ministry of Culture and the National Agency for the Territorial Cohesion⁶⁴. The former were targeted with emails containing a file named "Strategic Review"⁶⁵. In the case of the embassies, the attacks constituted in

⁵⁵ *Cyberattacks On Embassies, Threat Actor Using ChatGPT To Write Malware, and MMS Vulnerabilities*, community.f5.com/kb/security-insights/cyberattacks-on-embassies-threat-actor-using-chatgpt-to-write-malware-and-mms-vu/335426.

⁵⁶ Ibidem.

⁵⁷ *Cyberattacks On Embassies* (n 3).

⁵⁸ *Cyberattacks On Embassies* (n 4).

⁵⁹ *Cyberattacks On Embassies* (n 5).

⁶⁰ *Cyberattacks On Embassies* (n 6).

⁶¹ *Cyberattacks On Embassies* (n 10).

⁶² Wajahat Raja, *Russia APT Targets Storm- 0156 Server For Attack Campaigns*, (TuxCare) tuxcare.com/blog/alert-french-diplomats-targeted-by-russian-cyber-attacks/, 20th december 2024.

⁶³ Ibidem.

⁶⁴ *Russia APT Targets Storm* (n 1).

⁶⁵ ANSSI, *Malicious activities linked to the Nobelium intrusion set*, advisory, 19th of June 2024, page 1.

phishing email sent to public organizations⁶⁶. The emails were sent from the addresses of foreign institutions and individuals that were also victims of the same viruses⁶⁷. This created the perfect trap and raised no concern of the targeted institutions. For example, the French embassy in Kyiv received an email called “Diplomatic car for sale”, which contained the virus⁶⁸. As ANSSI stated, this particular attack was unsuccessful⁶⁹. However, the threat remains.

Another operation was designed against the Ministry of Foreign Affairs of France. The perpetrators were trying to install a tool named Cobalt Strike that was supposed to enable the remote control over the compromised infrastructure⁷⁰. However, this attack was also deemed unsuccessful. ANSSI also shows how the private accounts of diplomats can be hacked in order to trick other embassies and diplomatic structures to believe in the veracity of a certain attack. In March 2022, ANSSI documented that a European embassy in South Africa received an email announcing them that the French embassy was closing due to the threat of a terrorist attack⁷¹. The email was sent from a compromised account that belonged to a diplomat.

In fact, any informatics system can constitute a threat if not protected. Gadgets such as mobile phones, laptops and tablets can become a target for hackers. Smart TVs, smart vacuum cleaners or smart fridges can also become targets. The operating systems of airplanes, cars, trains are not safe either.⁷² Cyberattacks against these means of transportation can happen anywhere in the world, with minimum effort, through attacks that can be remotely conducted.⁷³

⁶⁶ thehackernews.com/2024/06/french-diplomatic-entities-targeted-in.html, 20th June 2024.

⁶⁷ Ibidem.

⁶⁸ ANSSI (n 1).

⁶⁹ ANSSI (n 2).

⁷⁰ ANSSI, *Malicious activities linked to the Nobelium intrusion set*, advisory, 19th of June 2024, page 2.

⁷¹ Ibidem.

⁷² Lev Topor, *Cyber sovereignty. International Security, Mass Communication, and the Future of the Internet*, Springer, 2024, page 84.

⁷³ Lev Topor (n 1).

2.2. Data Inviolability: the New Electronic Archives, Documents and Correspondence

This provision protects what can be resumed in one word: information. Naturally, information is of outmost importance in traditional diplomatic law, a view that the Tallinn Manual 2.0 shares.

Rule 41 of the Manual protects the inviolability of electronic archives, documents and correspondence⁷⁴. The main objective of this provision is to ensure the confidentiality of the information, a *sine qua non* condition to properly fulfill one's diplomatic duties.⁷⁵

The Manual highlights that this obligation can only belong to States, therefore private entities are excluded from the scope of this provision.⁷⁶ Establishing responsibility of such private entities can only be done by attributing their acts to a State.⁷⁷

The term *archive* has a broad meaning: it contains external hard drives, flash drives, USBs⁷⁸. *Documents* may include treaties and political documents, but also *notes verbales*, negotiation drafts etc.⁷⁹ Both of the notions require a wide interpretation. The same approach must be followed for *official correspondence*.

One particular question divided experts and fueled a fascinating debate: is diplomatic material in electronic form inviolable if it finds itself outside of the receiving State's territory?⁸⁰ Some experts believed that data could be protected by the inviolability of the mission.⁸¹ It can be observed that the two types of inviolabilities are complementary. Some experts adopted the view that such information, outside the premises, enjoys "absolute" inviolability⁸², the inviolability extending to third parties as well. Some even pointed out that this is a correct solution, considering how easy States can nowadays

⁷⁴ Tallinn Manual 2.0, rule 41.

⁷⁵ Tallinn Manual 2.0, page 219.

⁷⁶ Tallinn Manual 2.0, page 219.

⁷⁷ Tallinn Manual 2.0, page 219.

⁷⁸ Tallinn Manual 2.0, page 220.

⁷⁹ Ibidem.

⁸⁰ Ibidem.

⁸¹ Ibidem.

⁸² Ibidem.

access data outside their territory.⁸³To illustrate how electronic archives, documents and correspondence can be compromised, a practical example may be useful.

Canada is one of the States that suspected a foreign interference in their national elections from 2019 to 2021, which led to an intricate investigation.⁸⁴ The *Foreign Interference Commission* had the mandate to “examine and assess the interference by China, Russia and other foreign States or non-state actors, including any potential impacts”.⁸⁵ Moreover, it was mandated to analyze the flow of information between Canadian officials, in order to clearly identify the security breaches that caused the leakage of information.⁸⁶

The Commission issued its report in January 2025. The verifications have identified a group of “malicious cyber actors”, named APT 31 (“Advanced Persistent Threat 31”), acting under the direction of the Ministry of State Security of the People’s Republic of China (PRC).⁸⁷ At the time, APT 31 was targeting Canadian politicians, as they were part of a broader group, the Inter-Parliamentary Alliance on China (“IPAC”), whose members shared “the common value that China is a threat” to the security of their countries.⁸⁸

APT 31 sent spear phishing emails, imbedded with tracking links, to IPAC members.⁸⁹ Although the virus in itself was not able to compromise the device or the account of the victim, it was able to steal the user’s IP address and, consequently, lay the foundation of a series of subsequent cyber operation against the IPAC members.⁹⁰ The malicious links were sent both on the parliamentary and personal email addresses.⁹¹ In this way, APT 31 was able to keep track of the entire activity of the parliamentarians.

This example can be illustrative for the threats diplomats may face.

⁸³ Ibidem.

⁸⁴ Site of the *Foreign Interference Commission*, <https://foreigninterferencecommission.ca/>.

⁸⁵ Ibidem.

⁸⁶ Ibidem.

⁸⁷ Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *The Government’s Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 2/2)*, Volume 4, Chapters 14-18, Chapter 15, section 15.4, page 72.

⁸⁸ Ibidem.

⁸⁹ Ibidem.

⁹⁰ Ibidem.

⁹¹ Ibidem.

In their article *The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis*, the authors Nick Robinson, Laura Kask, Robert Krimmer question whether the Vienna Convention is able to protect the data and the information systems that are crucial parts of the diplomatic activity, by extending the protection conferred by the inviolability of the diplomatic mission to the data that is being stored in the clouds of a certain public administration⁹². Should the international community create new provisions in order to ensure the protection of data and information systems?

After the infamous cyberattack that occurred in Estonia in 2007, Estonian authorities decided to protect their data in one of the most interesting and innovative ways: creating a virtual embassy. It is a data center located in Luxembourg, “a digital continuity of Estonia as a state”.⁹³ The project emerged in 2015, when negotiations were initiated between Estonian representatives and Luxembourg’s authorities⁹⁴. A bilateral agreement was signed in 2017.⁹⁵

The Estonian embassy raises some interesting debates regarding its true legal nature. The virtual embassy functions on a dedicated server, a part of an already existing government-operated data center of the Estonian government⁹⁶. Certainly, the explanatory memorandum between Estonia and Luxembourg labels it as an “embassy”. However, this denomination may be challenging when applying the provisions of the Vienna Convention on Diplomatic Relations. In order to establish embassies, sending States must receive recognition from the receiving States⁹⁷. Moreover, these embassies need to be registered accordingly⁹⁸. Another difficulty lies in the fact that the data center does not have actual personnel that represents the Estonian state⁹⁹. If there are no diplomats, why should does premises enjoy special status in

⁹² Robinson N, Kask L and Krimmer R, *The Estonian Data Embassy and the Applicability of the Vienna Convention*, Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (2019), doi.org/10.1145/3326365.3326417.

⁹³ Estonia Data Embassy Fact Sheet, found on the site of the Data Embassy.

⁹⁴ Ibidem.

⁹⁵ Fact Sheet (n 1).

⁹⁶ Robinson N, Kask L and Krimmer R, *The Estonian Data Embassy and the Applicability of the Vienna Convention...*

⁹⁷ Ibid.

⁹⁸ The Estonian Data Embassy (n 1).

⁹⁹ The Estonian Data Embassy (n 2).

international law? These are important questions that have not been given an appropriate answer so far.

Conclusion

The Vienna Convention has constituted the cornerstone of diplomatic relations for decades. Despite its popularity and success in the international community, this convention couldn't have foreseen the new challenges that threaten to completely change international relations.

In the context of the growing importance of cyberspace, the experts that contributed to the Tallinn Manual 2.0 have established an important precedence for the development of the diplomatic inviolabilities. New conditions were added to the traditional provisions of the Convention, a sign to show that traditional diplomatic law doesn't cover these aspects in a sufficient matter. But are these steps enough? Should the international community solely rely on the general rules established by the Convention? If the answer is no, what exactly should these provisions contain, in order to navigate the intricate sphere of cyberspace?

The answers to these questions are far from simple, especially in a polarized world like the one we live in. However, one thing is certain: the subject of diplomatic inviolability in the tech era is crucial for the entirety of the diplomatic community and it will be necessary to address it in the following years. The need for a coordinated response is stringent. Such an important aspect cannot be addressed individually, but multilaterally, together with all the stakeholders involved in the development of cyberspace.

Bibliography

Books

- Behrens P, “Diplomatic Law in a New Millennium”, (Oxford University Press 2017).
- Denza Eileen, “Commentary on the Vienna Convention Diplomatic Relations. A commentary” (Oxford University Press 2008).
- Hauck SG, Kunz R and Milas M, “Public International Law: A Multi-Perspective Approach” (Taylor & Francis 2024).
- Riordan S, *Cyberdiplomacy: Managing Security and Governance Online* (John Wiley & Sons 2019).
- Schmitt MN, “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” (Cambridge University Press 2018).
- Shaw Malcolm, “International law. Ninth edition” (Cambridge University Press 2021).
- Xiaodong Yang, “State immunity in international law” (Ninth Edition, Cambridge University Press).

Articles

- Mallesons King & Wood, “China’s new foreign State immunity law- from absolute immunity to restrictive immunity” (<https://www.kwm.com/hk/en/insights/latest-thinking/China-new-foreign-state-immunity-law.html>).
- Felipe López-Valencia, “Diplomatic Shield: The Historical Origin and Dynamics of Diplomatic Immunity in Public International Law” (<https://dip.uexternado.edu.co/uncategorized/diplomatic-shield-the-historical-origin-and-dynamics-of-diplomatic-immunity-in-public-international-law/#:~:text=The%20roots%20of%20diplomatic%20immunity,suggests%20that%20messengers%20enjoyed%20protection>).
- K.A.A.N. Thilakarathna Akalanka, “The Evolution Of The Vienna Convention On Diplomatic Relations And Consular”, (file:///C:/Users/loana/Downloads/ajol-file-journals_479_articles_195181_submission_proof_195181-5653-493383-1-10-20200423.pdf, read on the 10th of January 2025).
- Lazăr Elena, *Jurisdiction et cybercriminalité*, Revue TIC, Innovation et droit international, Ed. Pedone, 2017
- Rene Vark, “Personal Inviolability and Diplomatic Immunity in Respect of Serious Crimes”, *Juridica International*, VIII/2013.
- Corneliu Bjola, Ilan Manor, “The rise of hybrid diplomacy: from digital adaptation to digital adoption”, *International Affairs* 98, 2022.
- Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, (https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf).
- Al-Muftah H, Weerakkody V, Rana NP, Sivarajah U, Irani Z., “Factors influencing e-diplomacy implementation: Exploring causal relationships using interpretative structural modelling”, *Government Information Quarterly*, (2018).

Conventions

Vienna Convention on Diplomatic Relations, 1961.

Vienna Convention on Consular Relations, 1963.

Vienna Convention on the Law of Treaties, 1969.

United Nations Convention on Jurisdictional Immunities of States and Their Property, 2004.

Other Sources

ANSSI, Malicious activities linked to the Nobelium intrusion set.

Council of Europe, “State immunity under International Law and Current Challenges”, CAHDI 2017, opening address of Mr. Martin Smolek, (<https://rm.coe.int/final-publication-state-immunity-under-international-law-and-current-c/16807724e9>).

ENISA, “Good Practice Guide for deploying Governmental Clouds”, page 4, <https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practice%20Guide%20for%20securely%20deploying%20Governmental%20Clouds.pdf>.

Permanent Council of the Organization of American States, Statement from the OAS General Secretariat on Events in Ecuador (https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-020/24).

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions, The Government’s Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 2/2).

United Nations Department of Economic and Social Affairs, United Nations E-Government Survey 2022, Chapter 5: The future of Digital Government: Trends, Insights and Conclusions.

United Nations, General Assembly, “Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation”, report of the Secretary-General (A/74/81), available at <https://www.un.org/en/content/digital-cooperation-roadmap/>.

United Nations Department of Economic and Social Affairs, United Nations E-Government Survey 2022.

United States Department of State, Office of Foreign Mission, “Diplomatic and Consular Immunity: Guidance for Law Enforcement and Judicial Authorities”, 2018.