-- The Quarterly Journal of Public Law Research ------
Summer 2026, 28 (91), 227- 284
qjpl.atu.ac.ir
DOI: 10.22054/qjpl.2025.83725.3067

ATU PRESS

Original Research
Received: 09/Jan/2025
Accepted: 03/June/2025
ISSN:2345-6116
eISSN:2476-6216

The Interaction of Diplomatic and Consular Law with Cyber Operations in Light of the Tallinn Manual 2.0

Kian Biglarbeigi — Ph.D. Student, International Law, Tehran University, Tehran, Iran

Sattar Azizi * — Faculty Member, Department of Law, Faculty of Humanities, Bu-Ali Sina University, Hamedan, Iran

1. Introduction

States, like individuals, do not exist in isolation; rather, they necessarily interact with one another. A state's geographical position requires it to maintain certain relations with neighboring states and different kinds of relations with others. One of the oldest expressions of friendly relations is diplomacy. Through diplomatic and consular relations, states generally conduct their foreign affairs. In other words, these relations reflect and embody the foreign policy and external

* Corresponding Author: s.azizi@basu.ac.ir
How to Cite: Biglarbeigi, K & Azizi S., "The Interaction of Diplomatic and Consular Law With Cyber Operations in Light of the Tallinn Manual 2.0", The Quarterly Journal of Public Law Research, Vol. 28, No. 91, (2026), 227-284. Doi: 10.22054/qjpl.2025.83725.3067

relations of international legal entities (i.e., states).

The Internet has become an essential tool for diplomatic negotiations and communication with a wide range of stakeholders. Nevertheless, the absence of treaty law and customary international law in the cyber domain is readily apparent. Still, a few attempts have been made to fill this gap. For example, the 2001 Budapest Convention on Cybercrime—concluded within the framework of the Council of Europe and its Additional Protocol—addresses only individual crimes. Perhaps the only relevant reference is the Tallinn Manuals, prepared in 2013 and 2017 by a group of international experts under NATO auspices

The absence of specific rules does not mean that states may conduct cyber operations without legal constraint. Although existing treaty laws and customary international law do not explicitly regulate cyber operations, established methods of legal interpretation make it possible to extend existing rules to this domain. This approach has been accepted by international organizations such as the United Nations and the European Union, as well as by a number of states, including the United States, Iran, the United Kingdom, Russia, Italy, Australia, China, the Netherlands, Qatar, Cuba, Hungary, and Mali.

The Tallinn Manual 2.0 is widely regarded as the most authoritative and frequently cited work on the international law applicable to cyber operations. Given the normative gap and the absence of uniform state practice, the Manual provides a comprehensive analysis of how existing international rules and regulations may be adapted to the complex and evolving domain of cyberspace. It also offers valuable insight into the views of legal and technical experts regarding how states engaged in cyber operations should conduct themselves.

Considering the rules and interpretations of Tallinn Manual 2.0, the present study aimed to examine the international law governing diplomatic and consular relations as it applies to state conduct in cyberspace.

2. Literature Review

Given the novelty of the topic, no research in Iran has yet examined the international law governing diplomatic and consular relations as it applies to state conduct in cyberspace. This distinguishes the present article in terms of its timeliness, theoretical framework, and analytical focus.

3. Materials and Methods

This study adopted a descriptive–analytical approach and drew on library sources to examine the positions advanced in the Tallinn Manual 2.0 in light of both general international law and the specific body of international law governing diplomatic and consular relations as applied to cyber operations. Accordingly, the study relied not only on the Tallinn Manual 2.0, but also on the 1961 Vienna Convention on Diplomatic Relations and the 1963 Vienna Convention on Consular Relations, since diplomatic and consular law is grounded primarily in these two conventions. The international group of experts involved in the preparation of the Tallinn Manual 2.0 also agreed that these conventions largely reflect customary international law.

4. Results and Discussion

The analysis first addressed the basic definitions and concepts relating to cyberspace and to diplomatic and consular law. Then it focused on

the conditions and requirements governing cyber operations within the framework of diplomatic and consular law. Communication is vital to diplomacy. The nature of the Internet has made it an indispensable tool for communication in the modern age and has given rise to what may be called *internet diplomacy*. Other factors contributing to this transformation include widespread access to telecommunications networks and the low cost of telecommunications equipment, both of which have expanded the capacity of many states to engage in internet diplomacy.

In this new environment, traditional diplomacy must evolve through the reinterpretation of existing rules, and where those rules prove inadequate or incomplete, new ones must be developed. First, diplomatic and consular missions enjoy the inviolability of their premises under customary international law, as codified in the Vienna Conventions on Diplomatic and Consular Relations. Mission premises are inviolable, and officials of the receiving state may not enter them without the consent of the head of mission.

Moreover, any property within the mission—including information and communication technology (ICT) infrastructure—is immune from search, seizure, confiscation, and the enforcement of judicial orders. This means that even remote access to ICT infrastructure located within the mission, without explicit consent, is prohibited. In addition, the mission's archives, documents, and official communications are inviolable, even in electronic form and regardless of their location. The receiving state is also obligated to ensure the mission's freedom of communication for all official purposes. All persons enjoying privileges and immunities are under an obligation to respect the laws and regulations of the receiving state and to refrain from interfering in its internal affairs.

Moreover, the premises of the mission must not be used in any manner incompatible with the functions of the mission, with general international law, or with any special agreement in force between the sending and receiving states.

In the cyber context, this means that persons enjoying privileges and immunities must not engage in unlawful surveillance or espionage in the receiving state, and mission premises must not be used for such purposes. Correspondingly, the receiving state is required to take all appropriate measures to protect the mission against intrusion or damage and to prevent any disturbance of the mission's peace or impairment of its dignity. Therefore, if a state becomes aware of malicious cyber activity targeting a diplomatic or consular mission within its territory, it must take all appropriate measures to protect the mission against that activity.

5. Conclusion

Cyberspace is continuously evolving, and with its high growth potential, any number of future developments are conceivable. Cyber diplomacy has now become an integral part of the daily life of diplomats and consuls. However, the absence of treaty instruments and customary international law in the cyber domain is very evident. Consequently, cyber operations in cyberspace pose questions and challenges for diplomatic and consular law. In this new environment, traditional diplomatic and consular law must evolve through the reinterpretation of existing rules. Where certain rules prove insufficient or incomplete in regulating internet diplomacy, new rules must be established. International rules concerning the inviolability of premises, the immunity of documents and archives, the freedom of official communication, tax exemptions, and immunity from

jurisdiction must be reinterpreted and applied in a manner consistent with the cyber-diplomatic environment. Moreover, new rules should be formulated to guarantee the immunity of the cyber diplomatic or consular bag.

Keywords: Diplomatic Law, Consular Law, Cyberspace, Cyber Operations, Tallinn Manual 2.0

-- فصلنامه علمی پژوهش حقوق عمومی ---------
دوره ۲۸، شماره ۹۱، تابستان ۱۴۰۵، ۲۲۷-۲۸۴
qjpl.atu.ac.ir
DOI: 10.22054/qjpl.2025.83725.3067

مقاله پژوهشی
تاریخ دریافت: ۱۴۰۳/۱۰/۲۰ تاریخ پذیرش: ۱۴۰۴/۰۳/۱۳
ISSN: ۲۳۴۵-۶۱۱۶ eISSN: ۲۴۷۶-۶۲۱۶

مواجهه حقوق دیپلماتیک و کنسولی با عملیات سایبری در پرتو راهنمای تالین ۲

کیان بیگلربیگی دانشجوی دکتری حقوق بین‌الملل، دانشگاه تهران، تهران، ایران

ستار عزیزی * عضو هیئت علمی گروه حقوق، دانشکده علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران

چکیده

دیپلماسی سایبری اکنون به بخش جدایی‌ناپذیر از زندگی روزمره دیپلمات‌ها و کنسول‌ها تبدیل شده است. با این حال، قواعد مدون حقوق دیپلماتیک و کنسولی سنتی بوده و با این فضای نوین، مواجهاتی چالش‌زا دارد. برای نمونه چه قواعدی بر عملیات سایبری در فضای سایبر مطابق با حقوق دیپلماتیک و کنسولی حاکم است؟ از سوی دیگر خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه فضای سایبر نیز بسیار مشهود است. البته فقدان قواعد خاص به این‌معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به عملیات سایبری نمایند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت در خصوص عملیات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد. در این راستا راهنمای تالین ۲ به‌عنوان یکی از تلاش‌های مهم در راستای قاعده‌مندسازی فضای سایبر شناخته می‌شود. این راهنما در هفتمین فصل خود در قالب شش قاعده، نکات و ملاحظاتی پیرامون ارتکاب عملیات سایبری در حقوق دیپلماتیک و کنسولی بیان می‌نماید. از این‌رو در این پژوهش با استفاده از روش توصیفی- تحلیلی و بهره‌گیری از منابع کتابخانه‌ای، سعی شده است مواضع راهنمای تالین ۲ را در تطابق با قواعد و مقررات موجود در حقوق بین‌الملل عام و حقوق بین‌الملل خاص (حقوق دیپلماتیک و کنسولی) با عملیات سایبری مورد مداقه قرار دهد.

واژگان کلیدی: حقوق دیپلماتیک، حقوق کنسولی، فضای سایبر، عملیات سایبری، راهنمای تالین ۲.

* نویسنده مسئول: s.azizi@basu.ac.ir

مقدمه

دولت‌ها هم مانند افراد، منفرد و منزوی نیستند بلکه به اقتضای احتیاج با هم روابط دارند. موقعیت جغرافیایی ایجاب می‌کند که یک دولت با دولت‌های همسایه خود نوعی روابط خاصی و با سایر دولت‌ها نوعی دیگر رابطه داشته باشد.[۱] لذا یکی از جلوه‌های دیرینه روابط دوستانه، روابط دیپلماتیک هستند. دولت‌ها در چارچوب روابط دیپلماتیک و کنسولی است که اغلب امور خارجی خود را با یکدیگر تنظیم می‌کنند. به دیگر سخن، این روابط به‌گونه‌ای مظهر و تجلی سیاست خارجی و روابط بیرونی شخصیت‌های حقوقی بین‌المللی یعنی دولت‌ها هستند.[۲]

تحول در دیپلماسی ممکن است شامل بهره‌گیری از پیشرفت‌های فناوری مانند اینترنت باشد. اینترنت به یک ابزار ضروری برای مذاکرات دیپلماتیک و ارتباطات با گروه‌های ذی‌نفع مختلف تبدیل شده است. در این محیط جدید، حقوق سنتی دیپلماسی و امور کنسولی نیز باید از طریق تفسیر جدید قواعد موجود تکامل یابد. اگر برخی از این قواعد برای تنظیم «دیپلماسی اینترنتی»[۳] ناکافی یا ناقص باشند، باید قواعد جدیدی وضع شوند. قواعد بین‌المللی در خصوص مصونیت اماکن، مصونیت اسناد و بایگانی‌ها، آزادی مکاتبات رسمی، معافیت‌های مالیاتی و مصونیت از صلاحیت قضایی باید به‌گونه‌ای جدید تفسیر و اعمال شوند تا با محیط دیپلماسی سایبری تطبیق یابند. علاوه بر این باید قواعد جدیدی برای مصونیت «کیسه دیپلماتیک یا کنسولی سایبری» ایجاد شود.[۴]

با این حال، خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه فضای سایبر نیز بسیار مشهود است. به استثنای کنوانسیون سال ۲۰۰۱ بوداپست، موضوع جرایم سایبری

---

۱. جواد صدر، *حقوق دیپلماتیک و کنسولی*، چاپ شانزدهم (تهران: مؤسسه انتشارات دانشگاه تهران، ۱۳۹۸) ص ۱.

۲. ابراهیم بیگ‌زاده، *حقوق بین‌الملل*، جلد دوم، *روابط تابعان*، چاپ اول (تهران: بنیاد حقوقی میزان، ۱۴۰۱) صص ۸۵۹-۸۶۰.

3. Internet Diplomacy.

4. Won-Mog Choi, *Diplomatic and Consular Law in the Internet Age* (Singapore: Year Book of International Law, 2006) at 117.

که در چارچوب «شورای اروپا»[1] منعقد گردید[2] و پروتکل الحاقی به آن[3] که صرفاً به جرایم افراد مربوط می‌شود، سند بین‌المللی مهم دیگری در حوزه عملیات سایبری موجود نیست و شاید تنها بتوان به راهنماهای تالین اشاره کرد که در سال ۲۰۱۳[4] و ۲۰۱۷[5] توسط جمعی از کارشناسان بین‌المللی در چارچوب سازمان ناتو تهیه گردیده‌اند.[6]

باید خاطرنشان نمود که فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به عملیات سایبری نمایند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت در خصوص عملیات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی

---

1. The Council of Europe.

2. Convention on Cybercrime (Budapest Convention), Council of Europe, European Treaty Series – No. 185., (2001), Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https://rm.coe.int/1680081561.

۳. این پروتکل در خصوص «لزوم جرم‌انگاری اقدام‌های نژادپرستانه و بیگانه‌هراسی که با استفاده از رایانه ارتکاب می‌یابند» است.

Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer System, (2003), Retrieved November 17, 2024 from https://rm.coe.int/168008160f .

۴. از ترکیب ۲۳ نفری این کارشناسان، ۹ نفر از ایالات متحده آمریکا بودند و کشورهای دارای قابلیت‌های سایبری یا کشورهای قربانی حملات سایبری مانند روسیه، ایران و چین نماینده‌ای در این مجموعه نداشتند که این امر انتقادات شدیدی را برانگیخت.

Rain Liivoja & Tim McCormack, "Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello (July 23, 2013)", Yearbook of International Humanitarian Law, Volume 15, 2013, U of Melbourne Legal Studies Research Paper No. 650, Available at: https://ssrn.com/abstract=2297159.

۵. راهنمای تالین ۱ در حقوق بین‌الملل قابل اعمال در نبردهای سایبری متعلق به بازه زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در کشور استونی است که توسط مایکل اشمیت در مورد مقررات حاکم بر اقدام‌ها و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبرد ناتو در ولز بریتانی، در قالب اصل ۴ پیمان ناتو تهیه شده است. به‌رغم پیوند راهنمای تالین ۲ با ناتو، در مقدمه این راهنما تصریح شده است که قواعد بیان شده در این راهنما، دیدگاه کشورهای متبوع کارشناسان تدوین‌کننده، ناتو یا مرکز عالی دفاع مشترک سایبری ناتو (CCDCOE) نیست؛ بلکه تنها محصول مطالعه مستقل کارشناسان و متخصصان تدوین‌کننده می‌باشد.

۶. کیان بیگلربیگی، حملات سایبری و نقض اصل عدم مداخله، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، به راهنمایی ابراهیم بیگ‌زاده، تهران، دانشگاه شهید بهشتی، دانشکده حقوق، (۱۴۰۲) ص ۲.

مانند سازمان ملل متحد، اتحادیه اروپا و دولت‌های متعدد از جمله ایالات متحده، ایران، بریتانیا، روسیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالی این نظریه را پذیرفته‌اند.[1] از این‌رو در خلأ هنجاری و رویه واحد دولتی، راهنمای تالین ۲ به‌عنوان معتبرترین و پراستنادترین اثر در زمینه حقوق بین‌الملل قابل اعمال بر عملیات سایبری، بررسی دقیقی از نحوه اعمال قواعد و مقررات بین‌المللی موجود[2] در تطابق با حوزه پیچیده و در حال تحول فضای سایبر ارائه می‌کند و می‌تواند به خوبی دیدگاه کارشناسان و اندیشمندان حقوقی و فنی آشنا با مسائل سایبری در مورد نحوه رفتار دولت‌ها که دست به ارتکاب عملیات سایبری می‌زنند، روشن سازد.[3]

---

1. Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014) at 19-22.

۲. راهنمای تالین ۲ بازتاب‌دهنده قواعد و مقرراتی است که در زمان تدوین این راهنما وجود داشته (Lex lata)؛ نه این‌که قواعد و مقررات جدیدی به گستره حقوق بین‌الملل بیفزاید و از اظهاراتی که منعکس‌کننده Lex ferenda باشد، اجتناب می‌کند.

David A. Wallace & Mark Visger, "Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community", Journal of Law & Cyber Warfare, Vol. 6, No. 2, (2018), at 19.

۳. در باب اهمیت راهنمای تالین ۲ می‌توان بیان داشت این راهنما، یک سند الزام‌آور قانونی نیست؛ بلکه تلاشی به‌دنبال قابلیت اجرای قواعد و مقررات موجود در حقوق بین‌الملل بر عملیات‌های سایبری و راهنمایی معتبر برای سیاست‌گذاران، رهبران نظامی و کارشناسان حقوقی می‌باشد که هدف آن، روشن کردن ابهامات قانونی پیرامون عملیات سایبری و ترویج فضای سایبر با ثبات‌تر و امن‌تر از طریق تشویق دولت‌ها به پایبندی به هنجارها و اصول بین‌المللی است. راهنمای تالین ۲ و قواعد آن، به‌دلایل متعددی می‌تواند به‌عنوان یک مرجع معتبر و راهنمایی قابل اعتماد برای دولت‌ها، کارشناسان حقوقی و سیاست‌گذاران در زمینه تحلیل و تفسیر عملیات سایبری مورد استفاده قرار گیرد که در زیر به برخی از آن‌ها اشاره می‌شود:

۱. راهنمای تالین ۲ در مقدمه خود تأکید می‌کند که هدف آن، تطبیق و اعمال قواعد موجود حقوق بین‌الملل بر عملیات سایبری است. این به آن‌معناست که کارشناسان تدوین‌کننده این راهنما، درصدد ایجاد قواعد جدید برای حوزه سایبر نبوده‌اند، بلکه تمرکز آن‌ها بر تطبیق و انطباق قواعد و مقررات موجود از جمله کنوانسیون‌ها و عرف‌های موجود در حقوق بین‌الملل با فضای درحال تحول سایبر است. این رویکرد سبب شده است تا دولت‌ها این راهنما را به‌عنوان یک تفسیر معتبر از حقوق بین‌الملل موجود در حوزه سایبر بپذیرند؛

۲. این راهنما حاصل بررسی‌های دقیق دو گروه از کارشناسان بین‌المللی است که شامل حقوقدانان، اساتید دانشگاه و متخصصان فنی می‌باشد. اگرچه در مقدمه راهنما به صراحت بیان شده است که قواعد این راهنما، بیانگر دیدگاه‌های کشورهای متبوع کارشناسان، ناتو یا مرکز عالی پدافند مشترک سایبری ناتو نیست، در انتخاب کارشناسان نیز به این نکته توجه شده است و متخصصانی از کشورهای غیرغربی همچون چین، بلاروس، ژاپن، تایلند و غیره در تدوین آن

لذا در این مقاله در پرتو قواعد و شرح راهنمای تالین ۲، حقوق بین‌الملل حاکم بر روابط دیپلماتیک و کنسولی که در خصوص رفتار دولت‌ها در فضای سایبر کاربرد دارد، بررسی می‌شود. همچنین در تدوین این مقاله، به‌طور گسترده بر معاهدات کنوانسیون وین ۱۹۶۱ درباره روابط دیپلماتیک و کنوانسیون وین ۱۹۶۳ درباره روابط کنسولی تکیه شده است؛ چراکه حقوق دیپلماتیک و کنسولی به‌طور عمده بر اساس این کنوانسیون‌ها استوار است. گروه بین‌المللی کارشناسان راهنمای تالین ۲ توافق داشتند که این معاهدات به‌طور قابل توجهی منعکس‌کننده حقوق بین‌الملل عرفی[۱] هستند.[۲]

بهره گرفته شده است. قواعد و تفاسیر این راهنما با اتفاق آرا بین متخصصان به تصویب رسیده که اعتبار حقوقی آن را تقویت می‌کند؛

۳. در فرآیند تدوین تالین ۲، وزارت امور خارجه هلند از طریق «روند لاهه» جلساتی را با بیش از ۵۰ کشور و سازمان بین‌المللی برگزار کرد. نظرات ارائه‌شده توسط این کشورها، در تکمیل و اصلاح برخی از بخش‌های متن تأثیرگذار بوده است. همین تعامل باعث شد که دولت‌ها بیشتر این راهنما را به‌عنوان یک مرجع معتبر در نظر بگیرند؛

۴. از آن‌جایی‌که بسیاری از تهدیدات و حملات سایبری در خارج از چارچوب مخاصمات مسلحانه رخ می‌دهند، راهنمای تالین ۲ شامل قواعد مربوط به عملیات سایبری، هم در خلال جریان یک مخاصمه مسلحانه و هم در زمان صلح می‌شود که این امر باعث افزایش کاربرد آن برای دولت‌ها شده است؛

۵. در تفسیر قواعد، نظرات مختلف از جمله دیدگاه‌های اقلیت و حتی دیدگاه‌هایی که از سوی هیچ‌یک از کارشناسان پذیرفته نشده ولی از سوی برخی دولت‌ها مطرح شده‌اند، آورده شده است. این شفافیت و جامعیت باعث شده که دولت‌ها بتوانند از این راهنما برای تحلیل حقوقی مسائل سایبری خود استفاده کنند؛

۶. بسیاری از قواعدی که در راهنمای تالین ۲ مطرح شده است به‌عنوان اصول حقوق بین‌الملل عرفی تلقی شده‌اند. این امر بدین معناست که حتی بدون معاهده خاصی، این اصول برای همه دولت‌ها الزام‌آور هستند (مگر در مواردی که یک دولت به‌عنوان «معترض مستمر» باشد). این ویژگی، قابلیت استناد آن را برای دولت‌ها تقویت کرده است.

International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation* (Cambridge University Press, 2017), at 1-6.

۱. برای مطالعه بیشتر در این خصوص مراجعه نمایید به؛

Jan Wouters, Sanderijn Duquet & Katrien Meuwissen, *The Vienna Conventions on Diplomatic and Consular Relations* (in Cooper, Andrew F., Heine, Jorge & Thakur, Ramesh (eds), The Oxford Handbook of Modern Diplomacy, 2013) at 393; United States of America v. Iran, United States Diplomatic and Consular Staff in Tehran, ICJ, Judgments, 1980, paras 62, 69. Retrieved January 3, 2025 from https://www.icj-cij.org/case/64.

2. Tallinn Manual 2.0, op.cit., at 209.

از سوی دیگر، حقوق حاکم بر سازمان‌های بین‌المللی به‌طور خاص در این مقاله مورد بحث قرار نگرفته است. سازمان‌های بین‌المللی عمده‌ای مانند سازمان ملل متحد[1] و آژانس‌های تخصصی آن، بر اساس معاهداتی که مزایا و مصونیت‌هایی مشابه با آن‌چه برای مأموریت‌های دیپلماتیک مقرر شده است دارند و از این حقوق بهره‌مند هستند. به‌عنوان مثال این سازمان‌ها از مصونیت اماکن و ارتباطات برخوردارند و نمایندگان این سازمان‌ها از مزایا و مصونیت‌هایی مشابه با آنچه به دیپلمات‌ها یا مأموران کنسولی اعطا می‌شود، بهره‌مند هستند. حقوق حاکم بر مزایا و مصونیت‌های اعطا شده به سازمان‌های بین‌المللی و کارکنان آن‌ها برای هر سازمان متفاوت است و در معاهدات تأسیسی یا سایر اسناد تشکیل‌دهنده سازمان‌ها همچنین در توافق‌نامه‌هایی که سازمان‌ها با دولت‌های میزبان و سایر دولت‌ها به‌منظور برخورداری از مزایا یا مصونیت‌ها برای انجام وظایف خود منعقد می‌کنند، یافت می‌شود.[2] به‌طور مشابه، حقوق حاکم بر مأموریت‌های ویژه به‌طورخاص در

---

۱. برای نمونه ماده ۱۰۵ منشور ملل متحد.

۲. برای‌نمونه کنوانسیون مزایا و مصونیت‌های سازمان ملل متحد ۱۹۴۶؛ توافق‌نامه بین سازمان ملل متحد و ایالات متحده در مورد مقر سازمان ملل متحد ۱۹۴۷؛ ماده ۴۸ اساسنامه دیوان بین‌المللی کیفری؛ توافق‌نامه مقر بین دیوان بین‌المللی کیفری و کشور میزبان ۲۰۰۷ را مشاهده نمایید. همچنین در این راستا دولت اتریش بیان داشته است: «حقوق و تعهدات مشابهی در زمینه سازمان‌های بین‌المللی اعمال می‌شود، تا جایی‌که این حقوق و تعهدات در توافق‌نامه‌های مقر بین دولت میزبان و سازمان بین‌المللی مشخص شده باشد. اماکن سازمان بین‌المللی غیرقابل تعرض هستند و ورود مأموران دولت میزبان به این اماکن تنها با رضایت رئیس سازمان بین‌المللی مجاز است. این امر همچنین شامل ممنوعیت دسترسی از راه دور به زیرساخت‌های فناوری اطلاعات و ارتباطات (ICT) واقع در اماکن سازمان بین‌المللی می‌شود. تمامی مقامات سازمان‌های بین‌المللی و نمایندگان دولت‌ها موظف به رعایت قوانین و مقررات دولت میزبان هستند و نباید در امور داخلی آن دولت مداخله کنند. این بدان معناست که این افراد نباید در فعالیت‌های نظارتی غیرقانونی یا جاسوسی در دولت میزبان شرکت کنند و اماکن سازمان بین‌المللی نباید برای چنین اهدافی مورد استفاده قرار گیرند. دولت‌های میزبان همچنین موظف به حفاظت از اماکن سازمان بین‌المللی در برابر اختلالات خارجی یا ورود غیرمجاز هستند. بنابراین اگر دولتی از یک فعالیت مخرب سایبری علیه یک سازمان بین‌المللی مستقر در قلمرو خود آگاه شود، باید تمامی اقدامات مناسب را برای حفاظت از آن سازمان در برابر چنین فعالیتی انجام دهد. در این راستا، اتریش به‌طور نزدیک با سازمان‌های بین‌المللی مستقر در قلمرو خود همکاری می‌کند».

Position Paper of the Republic of Austria: Cyber Activities and International Law, (2024), at 15. Retrieved January 3, 2025 from https:// docs-library.unoda.org/Open-Ended_ Working_ Group_ on_ Information_ and_ Communication_ Technologies_-

این مقاله مورد بررسی قرار نگرفته است. کنوانسیون ۱۹۶۹ درباره مأموریت‌های ویژه به مزایا و مصونیت‌هایی می‌پردازد که برای «مأموریت‌های ویژه» اعمال می‌شود، یعنی مأموریت‌های موقتی که نماینده یک دولت‌فرستنده در یک دولت‌پذیرنده هستند و با رضایت دولت‌پذیرنده برای رسیدگی به مسائل خاص یا انجام یک وظیفه مشخص تشکیل می‌شوند.[۱] اگرچه این کنوانسیون به‌طور گسترده تصویب نشده و تنها با رضایت دولت‌پذیرنده قابل اجرا است، کارشناسان راهنمای تالین ۲ اذعان داشتند که میان دولت‌ها حمایت از این موضع وجود دارد که اعضای مأموریت‌های ویژه به‌عنوان بخشی از حقوق

_ (2021)/ Austrian_ Position_ Paper_-_Cyber_ Activities_ and_ International_ Law_ (Final_23.04.2024).pdf.

۱. ماده ۱و ۸ کنوانسیون مأموریت‌های ویژه؛ ماده یک (معانی اصلاحات) بیان می‌دارد: «از لحاظ کنوانسیون حاضر؛ الف- اصطلاح «مأموریت ویژه» می‌شود به یک مأموریت موقت که به نمایندگی از طرف یک دولت با کسب موافقت قبلی دولت دیگر به‌منظور حل‌وفصل مسائل معین یا انجام وظایف معین نزد دولت اخیرالذکر اعزام می‌گردد؛ ب- اصطلاح «مأموریت دیپلماتیک دایمی» اطلاق می‌شود به مأموریت دیپلماتیک به مفهومی که در کنوانسیون وین درباره روابط دیپلماتیک تعریف شده است؛ ج- اصطلاح «پست کنسولی» اطلاق می‌شود به سرکنسولگری، کنسولگری، کنسولیاری، یا نمایندگی کنسولی؛ د- اصطلاح «رییس مأموریت ویژه» به شخصی اطلاق می‌شود که از طرف دولت فرستنده مأمور انجام وظیفه در این سمت می‌شود؛ ه- اصطلاح «رییس نماینده دولت فرستنده در مأموریت ویژه» به شخصی اطلاق می‌شود که دولت فرستنده این سمت را به او تفویض نموده باشد؛ و- اصطلاح «اعضاء مأموریت ویژه» اطلاق می‌شود به رییس مأموریت ویژه نمایندگان دولت فرستنده در مأموریت ویژه - و کارکنان مأموریت؛ ز- اصطلاح «کارمندان مأموریت ویژه» اطلاق می‌شود به کارمندان دیپلماتیک؛ کارمندان اداری و فنی؛ و خدمه مأموریت ویژه؛ ح- اصطلاح «کارمندان دیپلماتیک» اطلاق می‌شود به کارمندان مأموریت ویژه که از لحاظ مأموریت ویژه دارای مقام دیپلماتیک می‌باشند؛ ط- اصطلاح «کارمندان اداری و فنی» اطلاق می‌شود به کارمندان مأموریت ویژه که به امور اداری و فنی مأموریت ویژه اشتغال داشته باشند؛ ی- اصطلاح «خدمه» اطلاق می‌شود به کارکنان مأموریت ویژه که توسط مأموریت ویژه به‌عنوان خدمه منازل یا برای انجام کارهای‌مشابه استخدام شده باشند؛ ک- اصطلاح «خدمتکاران شخصی» اطلاق می‌شود به کسانی که منحصراً در خدمت شخصی اعضا مأموریت ویژه باشند». همچنین ماده هشتم (انتصاب اعضای مأموریت ویژه) مقرر می‌دارد: «دولت فرستنده می‌تواند با رعایت مقررات مواد ۱۰ و ۱۱ و ۱۲ و پس از آن‌که کلیه اطلاعات لازم درباره عده اعضا و ترکیب مأموریت ویژه و بالاخص اسامی و سمت اشخاص مورد نظر خود را در اختیار دولت پذیرنده قرار داد اعضای مأموریت ویژه را رأساً منصوب نماید. دولت پذیرنده می‌تواند از قبول مأموریت ویژه‌ای که عده اعضای آن را با توجه به امکانات و اوضاع‌واحوال خود و احتیاجات مأموریت ویژه متناسب تشخیص نمی‌دهد امتناع ورزد و نیز می‌تواند بدون ذکر دلیل از قبول شخص معینی به‌عنوان عضو مأموریت ویژه خودداری نماید».

بین‌الملل عرفی از مصونیت و غیرقابل تعرض بودن به‌ویژه با توجه به رویه دولت‌ها در اعطای مزایا و مصونیت‌های مقرر در کنوانسیون مأموریت‌های ویژه، برخوردارند. کارشناسان خاطرنشان کردند، هنگامی که مأموریت‌های ویژه از امکانات مأموریت‌های دیپلماتیک دولت خود استفاده می‌کنند، غیرقابل تعرض بودن اماکن و زیرساخت‌های سایبری مرتبط، فعالیت‌های سایبری آن‌ها را همان‌گونه که در فصل هفتم راهنمای تالین ۲ مورد بحث قرار گرفته است، صرف‌نظر از اعمال مزایا و مصونیت‌هایی که مأموریت‌های ویژه مستحق آن هستند، محافظت می‌کند.[1]

لذا در نهایت، این نوشتار در قالب دو گفتار تدوین شده است؛ در گفتار نخست ابتدا به تعاریف و مفاهیم کلی در حوزه سایبر و حقوق دیپلماتیک و کنسولی پرداخته سپس در گفتار دوم، شرایط و الزاماتی که بر عملیات سایبری در چارچوب حقوق دیپلماتیک و کنسولی بار می‌گردد؛ بررسی می‌شود.

۱. تعاریف و مفاهیم کلی

نظر به این‌که برای بررسی چارچوب حقوقی مواجهه حقوق دیپلماتیک و کنسولی با عملیات سایبری لازم است در ابتدا نسبت به این مفاهیم شناختی وجود داشته باشد، در این گفتار به‌صورت اجمالی، کلیاتی در خصوص این بررسی می‌شود.

۱-۱. سایبر و فضای سایبر

واژه سایبر از لغت یونانی (کی‌برنتز)[2] به‌معنی سکان‌دار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شده است. همچنین از این واژه به معنا و مفهوم مطالعه پیام‌ها به‌ویژه بررسی کنترل مؤثر در قلمرو فیزیولوژیک و مهندسی یاد می‌شود. اما به‌طور کلی فضای سایبر در اصل یک فضا و محیطی مشابه سایر حوزه‌های رقابتی همچون دریا، زمین و هوا است با یک تفاوت و

1. Tallinn Manual 2.0, op.cit., at 211.
2. Kybernetes.

آن‌هم این‌که این محیط برخلاف بقیه محیط‌ها ساخته دست بشر بوده، غیرملموس است[۱] و منبعی برای تبادل اطلاعات تلقی می‌شود.

۲-۱. عملیات و فعالیت سایبری

اصطلاحات «عملیات سایبری»[۲] و «فعالیت سایبری»[۳] مفاهیم عامی هستند و بسته به سیاق متن ممکن است معانی متفاوتی داشته باشند، ولی در این نوشتار به‌جای یکدیگر به‌کار رفته‌اند. چنانچه بخواهیم تعریفی یکپارچه از این دو اصطلاح ارائه دهیم، می‌توان گفت انواع مختلفی از فعالیت‌ها هستند که از فضای سایبر با هدف تأثیرگذاری بر اطلاعاتی که در قلمرو سایبری جریان دارند، استفاده می‌شوند.[۴]

۳-۱. دولت‌پذیرنده و فرستنده

اصطلاح «دولت‌پذیرنده» به دولتی اشاره دارد که یک مأموریت دیپلماتیک یا پست کنسولی در آن اعتبارنامه دریافت کرده است. «دولت فرستنده» به دولتی اطلاق می‌شود که مأموریت یا پست پیش‌گفته نمایندگی آن را بر عهده دارد. لازم به ذکر است که دولت فرستنده می‌تواند پس از اعلام رسمی به دولت‌های ذی‌نفع، یک رییس مأموریت را برای نمایندگی خود نزد چند دولت و همچنین یکی از کارمندان دیپلماتیک خود را برای انجام وظایف مربوط نزد دولت‌های متعدد بگمارد، مگر آن‌که یکی از آن دولت‌ها صریحاً با این امر مخالفت ورزد.[۵] در چنین مواردی، منظور از اصطلاح «دولت پذیرنده» تمامی دولت‌هایی است که فرد نزد آن‌ها به‌عنوان نماینده (مأمور) اعتبارنامه دریافت کرده یا به آن‌ها آکردیته شده است.

---

1. Martin C Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009) at 11.
2. Cyber Operations.
3. Cyber Activities.
4. Tallinn Manual 2.0, op.cit., at 564.
۵. ماده ۵ کنوانسیون روابط دیپلماتیک.

۱-۴. مأموریت، اماکن و نماینده دیپلماتیک

اصطلاح «مأموریت دیپلماتیک» به حضور دیپلماتیک یک دولت در دولت دیگر اشاره دارد که با رضایت دولت دوم تأسیس شده و با هدف نمایندگی دولت فرستنده در دولت پذیرنده و انجام سایر وظایف مقرر در حقوق بین‌الملل فعالیت می‌کند. «اماکن مأموریت» به «ابنیه و یا بخش‌هایی از آن‌ها، زمین متعلق به آن، که صرف‌نظر از مالکیتشان برای انجام اشتغالات مأموریت دیپلماتیک به‌کار می‌روند و محل اقامت رئیس مأموریت» اطلاق می‌شود.[۱] «نماینده دیپلماتیک» به رئیس مأموریت یا عضوی از کارکنان دیپلماتیک مأموریت اشاره دارد.[۲]

۱-۵. پست، امکان و مأمور کنسولی

«پست کنسولی» به هرگونه سرکنسولگری، کنسولگری، کنسولیاری یا نمایندگی کنسولی یک دولت فرستنده در یک دولت پذیرنده اشاره دارد که با رضایت دولت پذیرنده تأسیس شده و با هدف انجام وظایف کنسولی فعالیت می‌کند.[۳] «اماکن کنسولی» به «ابنیه و یا قسمت‌هایی از ابنیه و زمین متصل به آن، که مالک آن هرکه باشد - منحصراً برای انجام مقاصد پست کنسولی مورد استفاده قرار می‌گیرد» اطلاق می‌شود.[۴] «مأمور کنسولی» به «هر شخصی (منجمله رئیس پست کنسولی) که در این سمت عهده‌دار انجام وظایف کنسولی است» اشاره دارد.[۵] مأموران کنسولی ممکن است تحت شرایط خاص مجاز به انجام اقدامات دیپلماتیک شوند، اما انجام چنین اقداماتی به آنان حقی برای مطالبه مزایا و مصونیت‌های دیپلماتیک اعطا نمی‌کند.[۶]

---

۱. ماده ۱ (ط) کنوانسیون روابط دیپلماتیک.

۲. همان، ماده ۱ (الف)، (د) و(ه) کنوانسیون روابط دیپلماتیک.

۳. همان، ماده ۱ (۱) (الف) کنوانسیون روابط کنسولی.

۴. همان، ماده ۱ (۱) (ی) کنوانسیون روابط کنسولی.

۵. همان، ماده ۱ (۱) (د) کنوانسیون روابط کنسولی.

۶. همان، ماده ۱۷ کنوانسیون روابط کنسولی؛ قاعده ۴۴ راهنمای تالین ۲.

۲. شرایط و الزامات عملیات سایبری از منظر حقوق دیپلماتیک و کنسولی

ارتباطات برای دیپلماسی حیاتی است. ماهیت اینترنت آن را به ابزاری ضروری برای ارتباطات در این عصر مدرن تبدیل کرده و موجب ظهور پدیده‌ای شده که آن را «دیپلماسی اینترنتی» می‌نامیم. عوامل دیگری که به این تحول کمک کرده‌اند، از جمله دسترسی گسترده به ارتباطات مخابراتی و در دسترس بودن تجهیزات مخابراتی با قیمت‌های پایین هستند که ظرفیت بسیاری از کشورها را برای مشارکت در دیپلماسی اینترنتی افزایش می‌دهند.[۱] با این حال، عملیات سایبری در فضای سایبر، حقوق دیپلماتیک و کنسولی را با سؤال‌ها و چالش‌هایی روبرو می‌سازد. از این‌رو در ادامه، عملیات سایبری از منظر حقوق دیپلماتیک و کنسولی در شش بخش، مطابق راهنمای تالین ۲ مورد مداقه قرار می‌گیرد.

پیش از آن باید اشاره داشت، همان‌طور که کارشناسان راهنمای تالین ۲ خاطرنشان کردند؛ ارتباط میان حقوق دیپلماتیک و کنسولی با قواعد حقوق مسئولیت بین‌المللی دولت‌ها در مواردی که شرایط مانع از عمل متخلفانه می‌شوند،[۲] به‌ویژه پیچیده است. به‌طور خاص کارشناسان توافق داشتند همان‌طور که در قاعده ۲۲ راهنمای تالین ۲ آمده است،[۳] اقدامات متقابلی که موجب نقض غیرقابل تعرض بودن (از جمله مصونیت قضایی) مأموران دیپلماتیک یا کنسولی[۴]، اماکن[۵] یا آرشیو و اسناد[۶] شود، ممنوع است.[۷] به‌عنوان مثال اگر دولت فرستنده از زیرساخت سایبری یک مأموریت دیپلماتیک برای انتقال بدافزارهای جاسوسی به رایانه‌های دولت پذیرنده استفاده کند، چنین اقدامی سوءاستفاده از وظیفه

---

1. Choi, op.cit., at 118.

۲. قاعده ۱۹ راهنمای تالین ۲.

۳. قاعده ۲۲ راهنمای تالین ۲: «اقدام‌های متقابل، چه ماهیت سایبری داشته یا نداشته باشد، نمی‌تواند شامل اقدام‌هایی باشد که بر حقوق اساسی بشر تأثیر می‌گذارد، به تلافی‌جویی‌های ستیزه‌جویانه ممنوع یا ناقض هنجارهای آمرانه می‌شود. کشوری که اقدام‌های متقابل انجام می‌دهد، باید تعهدات خود را در رابطه با مصونیت دیپلماتیک و کنسولی انجام دهد».

۴. همان، قاعده ۴۴ راهنمای تالین ۲.

۵. همان، قاعده ۳۹ راهنمای تالین ۲.

۶. همان، قاعده ۴۱ راهنمای تالین ۲.

۷. ماده ۵۰ (۲) (ب) پیش‌نویس مواد راجع به مسئولیت دولت‌ها برای افعال متخلفانه بین‌المللی ۲۰۰۱ و بندهای ۱۴ و ۱۵ تفسیر کنوانسیون.

دیپلماتیک[۱] و بنابراین یک عمل متخلفانه بین‌المللی است.[۲] با این حال، دولت پذیرنده مجاز نیست به‌عنوان اقدام متقابل، عملیات سایبری علیه زیرساخت سایبری واقع در اماکن دیپلماتیک انجام دهد.[۳] همچنین کارشناسان توافق کردند که بر اساس اصل عمل متقابل[۴]، در صورتی‌که مأموریت یا پست آن دولت در دولت فرستنده با رفتاری مشابه مواجه شده باشد دولت پذیرنده می‌تواند در ارتباط با فعالیت‌های سایبری دولت فرستنده، رفتاری کمتر مطلوب در مقایسه با دیگر دولت‌های فرستنده نشان دهد. با این‌حال، آنها هشدار دادند که دولت‌پذیرنده نباید به‌گونه‌ای عمل کند که ناقض حقوق دیپلماتیک یا کنسولی باشد.[۵] کارشناسان به دیدگاهی اشاره کردند که هیچ‌یک آن را نپذیرفتند؛ این دیدگاه بیان می‌کند، دولتی که برخلاف مقررات حقوق دیپلماتیک یا کنسولی عمل کند، ممکن است با انکار متقابل حقوق به شکلی متناسب مواجه شود.[۶]

همچنین همان‌طورکه کارشناسان توافق داشتند، مواردی که در ادامه مقاله مورد مداقه قرار می‌گیرد، به‌طور کلی در زمان مخاصمات مسلحانه نیز اعمال می‌شود.[۷] در این رابطه، بند (الف) ماده ۴۵ کنوانسیون وین درباره روابط دیپلماتیک مقرر می‌دارد: «دولت‌پذیرنده حتی در صورت وقوع مخاصمه مسلحانه، موظف است اماکن مأموریت، همراه با اموال و آرشیوهای آن را محترم شمرده و از آن محافظت کند». بند (الف) ماده ۲۷ (۱) کنوانسیون وین درباره روابط کنسولی نیز حفاظت مشابهی را برای اماکن، اموال و آرشیوهای کنسولی مقرر می‌دارد. علاوه بر این، هر دو سند بیان می‌کنند وظایف افرادی که از مزایا و

---

۱. ماده ۳ (۱) کنوانسیون روابط دیپلماتیک.

۲. قاعده ۱۴ راهنمای تالین ۲.

3. Tallinn Manual 2.0, op.cit., at 211-212.

4. Reciprocity.

۵. رجوع نمایید به ماده ۴۷ (۲) کنوانسیون روابط دیپلماتیک؛ ماده ۷۲ (۲) کنوانسیون روابط کنسولی؛

Eileen Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations,* 4th Edition (Oxford: Commentaries on International Law, 2016) at 406–408.

6. Tallinn Manual 2.0, op.cit., at 212.

7. Ibid.

مصونیت‌های دیپلماتیک برخوردارند، در زمان مخاصمه مسلحانه ادامه دارد تا زمانی‌که شخص، کشور پذیرنده را ترک کند یا مهلت معقول برای این کار منقضی شود.[۱]

۱-۲. غیرقابل تعرض بودن اماکنی که زیرساخت سایبری در آن قرار دارد

غیرقابل تعرض بودن اماکن مأموریت دیپلماتیک یکی از اصول بنیادین حقوق دیپلماتیک است. بر اساس این اصل، اماکن مأموریت بدون رضایت رئیس مأموریت قابل ورود نیستند.[۲] بنابراین، مأموران دولت پذیرنده علی‌الاصول نمی‌توانند به هیچ بهانه‌ای بدون اجازه رئیس مأموریت وارد اماکن دیپلماتیک شوند. با این حال در موارد متعددی نقض اماکن مأموریت مشاهده می‌شود. این نقض مصونیت می‌تواند ناشی از ورود غیرمجاز نیروهای نظامی، انتظامی، وابستگان به فرد یا سازمان، گروه‌های انقلابی، شورشیان و مردم عادی انجام شود. شکل دیگری از نقض مصونیت اماکن مأموریت را می‌توان در قالب قراردادن تجهیزات و یا نصب دستگاه‌ها در دیوارها و یا داخل اماکن مأموریت یا محل اقامت دیپلمات‌ها برای شنود مکالمات و غیره مشاهده نمود.[۳]

در این راستا قاعده ۳۹ راهنمای تالین ۲ بیان می‌دارد: «زیرساخت سایبری موجود در اماکن مأموریت دیپلماتیک یا پست کنسولی، تحت حفاظت غیرقابل تعرض بودن آن مأموریت یا پست قرار دارد». این قاعده به اماکن پست کنسولی نیز تسری می‌یابد، اما حفاظت تنها شامل بخش‌هایی است که منحصراً برای اهداف پست کنسولی مورد استفاده قرار می‌گیرند.[۴]

در خصوص اجرای این قاعده، کارشناسان راهنمای تالین ۲ در مورد مشروعیت نفوذ از راه دور به زیرساخت سایبری موجود در اماکن دیپلماتیک یا کنسولی یک دولت - فرستنده یا اختلال یا تغییر داده‌ها در آن، اختلاف‌نظر داشتند. اکثریت کارشناسان معتقدند که این قاعده، دولت پذیرنده را از انجام چنین عملی منع می‌کند؛ چراکه عملیات سایبری

---

۱. ماده ۳۹ (۲) کنوانسیون روابط دیپلماتیک؛ ماده ۵۳ (۳) کنوانسیون روابط کنسولی.

۲. ماده ۲۲ (۱) کنوانسیون روابط دیپلماتیک.

۳. بیگ‌زاده، پیشین، ص ۸۸۴

۴. ماده ۳۱ کنوانسیون روابط کنسولی.

که بر روی زیرساخت سایبری در اماکن انجام می‌شود، به‌منزله ورود بدون رضایت به آن اماکن است. نتیجه‌گیری کارشناسان از این دیدگاه به‌ویژه با توجه به وظیفه ویژه دولت-پذیرنده در برداشتن تمام اقدامات مناسب برای حفاظت از اماکن مأموریت دیپلماتیک در برابر هرگونه نفوذ یا آسیب[۱] و همچنین الزام آن به تسهیل کامل عملکرد مأموریت، تقویت می‌شود.[۲ و۳] با این حال برخی از کارشناسان بر این باور بودند که نقض این قاعده مستلزم حضور فیزیکی دولت پذیرنده در مأموریت یا پست است. برای این افراد، انجام عملیات سایبری با دسترسی محدود[۴] به‌عنوان مثال می‌تواند این استاندارد را برآورده کند. آن‌ها همچنین مایل بودند که ایجاد پیامدهای فیزیکی از راه دور[۵] در یک مأموریت دیپلماتیک یا پست کنسولی را به‌عنوان نقض این قاعده تلقی کنند. تا جایی‌که این قاعده اماکن مأموریت‌های دیپلماتیک را در برابر ورود فیزیکی بدون رضایت محافظت می‌کند، برای این کارشناسان، ایجاد پیامدهای فیزیکی از راه دور، به‌طور مؤثر معادل حضور فیزیکی در آن اماکن است. البته باید هشدار داد فعالیت‌هایی که از راه دور علیه زیرساخت سایبری یک مأموریت دیپلماتیک یا پست کنسولی انجام می‌شود یا فعالیت‌های مشابه، ممکن است قواعد دیگری که در فصل هفتم راهنمای تالین ۲ مقرر شده است مانند قاعده مربوط به حفاظت از آرشیوهای دیپلماتیک، اسناد و مکاتبات رسمی[۶] نقض کنند. به‌عبارت دیگر این‌که عملیات سایبری دولت‌پذیرنده نقض این قاعده نباشد، لزوماً به این معنا نیست که آن عملیات تحت حقوق دیپلماتیک و کنسولی قانونی باشد.[۷]

همچنین کارشناسان راهنمای تالین ۲ در مورد این‌که آیا دولتی غیر از دولت پذیرنده موظف است به غیرقابل تعرض بودن اماکن یک مأموریت دیپلماتیک یا پست کنسولی واقع در دولت پذیرنده احترام بگذارد یا نه؟ اختلاف‌نظر داشتند. به‌عنوان مثال فرض کنید

---

۱. ماده ۲۲ (۲) کنوانسیون روابط دیپلماتیک؛ قاعده ۴۰ راهنمای تالین ۲.

۲. ماده ۲۵ کنوانسیون روابط دیپلماتیک.

3. Denza, op.cit., at 171-172.

4. Close-Access.

5. Remote Causation of Physical Consequences.

۶. قاعده ۴۱ راهنمای تالین ۲.

7. Tallinn Manual 2.0, op.cit., at 213-214.

دولت «الف» یک عملیات سایبری برای استخراج داده‌ها از زیرساخت سایبری سفارت دولت «ب» در کشور «ج» انجام می‌دهد تا موقعیت‌های پرسنل دیپلماتیک دولت «ب» را تعیین کند. کارشناسان در مورد این مثال به‌طور مساوی تقسیم شدند. برخی از کارشناسان بر این باور بودند که دولت «الف» این قاعده را نقض کرده است و اشاره کردند که رفتار آن مغایر با موضوع و هدف اصل غیرقابل تعرض بودن است، همچنین این‌که دسترسی از راه دور به زیرساخت‌های سایبری به‌طور فزاینده‌ای یک مسئله صرفاً فنی است. در مقابل، سایر کارشناسان موضع مخالف را اتخاذ کردند و دلیل آن را این دانستند که تعهدات حقوقی در حقوق دیپلماتیک عمدتاً از روابط میان دولت‌های فرستنده و پذیرنده ناشی می‌شود. آن‌ها همچنین اشاره کردند که تعهدات خاصی که در متون معاهدات مربوط برای طرف‌های ثالث وضع‌شده، معمولاً به غیرقابل تعرض بودن مکاتبات و ارتباطات رسمی که در حال انتقال هستند[۱] محدود می‌شود.[۲] با این حال از نظر نگارندگان، این موضوع بحث مراقبت مقتضی[۳] در حقوق بین‌الملل را مطرح می‌نماید. مطابق قاعده ۶ راهنمای تالین ۲؛ یک دولت باید مراقبت مقتضی نماید تا اجازه ندهد از قلمرو یا زیرساخت‌های سایبری تحت کنترل دولتی‌اش برای عملیات سایبری استفاده شود که بر حقوق سایر کشورها تأثیر می‌گذارد و پیامدهای نامطلوب جدی برای آن‌ها به همراه دارد. در ادامه، قاعده ۷ نیز مقرر می‌دارد: «اصل مراقبت مقتضی از یک دولت می‌خواهد که تمام اقدام‌هایی را که در این شرایط امکان‌پذیر است برای پایان‌دادن به عملیات سایبری که بر حقوق سایر کشورها تأثیر می‌گذارد و عواقب نامطلوب جدی برای آن‌ها ایجاد می‌کند، اتخاذ کند» و همچنین از آن‌جایی‌که به‌ویژه با توجه به وظیفه ویژه دولت پذیرنده، در برداشتن تمام اقدامات مناسب

---

۱. رجوع نمایید به ماده ۴۰ (۱) و (۳) کنوانسیون روابط دیپلماتیک؛ ماده ۵۴ (۱) و (۳) کنوانسیون روابط کنسولی؛ قاعده ۴۱ راهنمای تالین ۲.

2. Tallinn Manual 2.0, op.cit., at 214.

۳. اصطلاح مراقبت مقتضی در لغت، به معنای مراقبت یا احتیاط منطقی است. در مفهوم حقوقی، به معنای مراقبت و هوشیاری است که به‌طور منطقی از کسی انتظار می‌رود و عرفاً در اوضاع و احوال خاصی از سوی فرد متعارفی که به دنبال اجرای تعهد حقوقی است انجام می‌پذیرد.

Bryan A Garner, *Black's Law Dictionary*, 8th Edition (USA: Thomson West, 1990) at 488.

برای حفاظت از اماکن مأموریت دیپلماتیک در برابر هرگونه نفوذ یا آسیب و همچنین الزام آن به تسهیل کامل عملکرد مأموریت، باید در صورت آگاهی[1] و توانایی لازم، در راستای مقابله با این عملیات به‌طور مناسب برآید.[2]

از سوی دیگر، کارشناسان توافق کردند که در شرایط اضطراری[3]، دولت پذیرنده ممکن است در دفاع از خود اقداماتی علیه اماکن یا زیرساخت سایبری موجود در یک مأموریت دیپلماتیک یا پست کنسولی انجام دهد.[4] به‌عنوان مثال اگر از زیرساخت سایبری موجود در یک مأموریت برای انتقال اطلاعات حیاتی درباره نیروهای مسلح دولت پذیرنده به‌منظور استفاده در یک حمله مسلحانه قریب‌الوقوع از سوی دولت فرستنده استفاده شود، دولت پذیرنده می‌تواند عملیات‌هایی را از جمله استفاده از آستانه توسل به زور علیه آن زیرساخت سایبری انجام دهد.[5] این امر بر این اساس توجیه می‌شود که حق دفاع مشروع به‌عنوان یک عامل رافع مسئولیت می‌تواند نقض تعرض‌ناپذیری اماکن دیپلماتیک و کنسولی را موجه سازد.[6] همچنین کارشناسان به دیدگاهی اشاره کردند که هیچ‌یک از آنان آن را نپذیرفتند، دائر بر این‌که غیرقابل تعرض بودن اماکن مأموریت یا پست مطلق است. حامیان این دیدگاه معتقدند که راه‌حل‌های موجود برای دولت پذیرنده در چنین شرایطی، همان راه‌حل‌هایی است که در حقوق دیپلماتیک و کنسولی مانند خاتمه یا تعلیق روابط دیپلماتیک یا کنسولی و همچنین استفاده از زور در دفاع از خود علیه اهداف غیر از اماکن مأموریت، پیش‌بینی شده است.[7]

---

1. Knowledge.

۲. برای مطالعه بیشتر رجوع نمایید به؛ بیگلربیگی، پیشین، ص ۱۱۶ به بعد.

3. Extremis.

۴. راهنمای تالین ۲ اشاره می‌نماید برای مطالعه بیشتر رجوع نمایید به قاعده ۷۱ راهنمای تالین ۲؛

Anthony Kershaw, *First Report from the Foreign Affairs Committee, Session 1984–85: the Abuse of Diplomatic Immunities and Privileges* (in Great Britain, Parliament, House of Commons, Foreign Affairs Committee, H.M. Stationery Office, 1984), Paras 88–95; International Law Commission, *Yearbook of the International Law Commission,* Vol. II (United Nations, 1958) at 97; Denza, op.cit., at 223.

5. Tallinn Manual 2.0, op.cit., at 214.

۶. ماده ۲۱ پیش‌نویس مواد راجع به مسئولیت دولت‌ها برای افعال متخلفانه بین‌المللی ۲۰۰۱.

7. Ibid. at 214.

علاوه بر این، پرسش جداگانه‌ای وجود دارد که به حفاظت از اموال یک مأموریت دیپلماتیک که در داخل اماکن آن نیست مانند تلفن‌های همراه رسمی یا لپ‌تاپ‌هایی که از اماکن خارج شده‌اند، مربوط می‌شود.

کارشناسان راهنمای تالین ۲ در این مورد نیز تقسیم شدند. اکثریت کارشناسان بر این باور بودند که چنین اموالی تحت این قاعده از غیرقابل تعرض بودن برخوردارند. بیشتر کارشناسان این اکثریت معتقد بودند که این اموال غیرقابل تعرض هستند. بنابراین، دولت فرستنده نمی‌تواند عملیات سایبری علیه آن انجام دهد. برای این کارشناسان، گسترش غیرقابل تعرض بودن به اموالی که خارج از اماکن مأموریت قرار دارند، با موضوع و هدف قاعده‌ای که به حفاظت از غیرقابل تعرض بودن دیپلماتیک و کنسولی مربوط می‌شود، هماهنگ است. آن‌ها اشاره کردند که چنین اموالی احتمالاً می‌توانند به‌عنوان «آرشیوهای»[1] غیرقابل تعرض مأموریت دیپلماتیک تحت قاعده ۴۱ شناخته شوند، زیرا معمولاً موارد دیپلماتیک رسمی بر روی آن‌ها ذخیره می‌شود.

در نهایت، کنوانسیون وین درباره روابط دیپلماتیک مقرر می‌کند که اموال شخصی متحرک مأموران دیپلماتیک غیرقابل تعرض، مشروط به استثنائات برای برخی اقدامات مدنی یا اداری هستند.[2] بنابراین برای این کارشناسان، نتیجه‌گیری دائر بر این‌که اموال یک مأموریت دیپلماتیک پس از خروج از اماکن قابل تعرض است، در حالی‌که اموال خصوصی یک مأمور دیپلماتیک که هر کجا قرار داشته باشد غیرقابل تعرض است، غیرمنطقی به‌نظر می‌رسد. از سوی دیگر برخی از کارشناسان از میان اکثریت، نتیجه‌گیری کردند که چنین اموالی تنها از عملیات‌های سایبری که موجب تفتیش، مصادره، توقیف یا اجرایی احکام قضایی شوند، مصون هستند. آن‌ها دیدگاه خود را بر اساس این حقیقت بنا کردند که اموال موجود در اماکن دیپلماتیک از این اشکال حفاظت برخوردارند.[3] این کارشناسان همچنین اشاره کردند که کنوانسیون وین درباره روابط دیپلماتیک همان

---

1. Archives.

۲. ماده ۳۰ (۲) کنوانسیون روابط دیپلماتیک؛

Yearbook of the International Law Commission, op.cit., at 98.

3. ماده ۲۲ (۳) کنوانسیون روابط دیپلماتیک.

مصونیت را به وسایل نقلیه نیز گسترش می‌دهد[۱] که یکی از اشکال اصلی اموال متحرک در زمان تصویب آن بود. آن‌ها همچنین به روند نوظهور شناسایی مصونیت از توقیف حساب‌های بانکی دیپلماتیک اشاره کردند.[۲] چند نفر از کارشناسان که با موضع اکثریت موافق نبودند، بر این باور بودند که چنین اموالی تحت این قاعده اصلاً از حفاظت برخوردار نیستند و به زبان کنوانسیون وین درباره روابط دیپلماتیک اشاره کردند که مصونیت از تفتیش، مصادره، توقیف یا اجرای احکام قضایی را تنها برای «اماکن مأموریت، اثاثیه آن و سایر اموال موجود در آن» فراهم می‌کند.[۳] در نهایت با توجه به پیچیدگی مسئله اموال خارج از اماکن مأموریت‌های دیپلماتیک، کارشناسان نتوانستند به نتیجه‌ای در خصوص اموال خارج‌شده از پست‌های کنسولی دست یابند.[۴ و ۵]

در پایان، کارشناسان راهنمای تالین ۲ اعلامیه‌های برخی از کشورها دائر بر ایجاد «سفارت‌های مجازی»[۶] را مورد بررسی قرار دادند. به‌عنوان مثال ایالات متحده وب‌سایت‌هایی راه‌اندازی کرده است که به آن‌ها «سفارت‌های مجازی» در ایران و سوریه

---

۱. ماده ۲۲ (۳) کنوانسیون روابط دیپلماتیک.

۲. برای نمونه به کنوانسیون سازمان ملل متحد در خصوص مصونیت‌های قضائی دولت‌ها و اموال آن‌ها رجوع نمایید. همچنین راهنمای تالین ۲ به موارد زیر اشاره می‌نماید؛

Alcom v. Republic of Colombia, House of Lords, 1984. Retrieved January 4, 2025 from https://vlex.co.uk/vid/alcom-ltd-v-republic-792878269; Republic of 'A' Embassy Bank Account Case, Supreme Court (Austria), (1986). Retrieved January 4, 2025 from https:// www. cambridge. org/ core/ journals/ international- law-reports/article/abs/republic-of-a-embassy-bank-account-case/D34423E41E557EAE87C9E2E98E7CE707; MK v. State Secretary for Justice, Council of State, President of the Judicial Division, 1988. Retrieved January 4, 2025 from http://www.cahdidatabases.coe.int/Contribution/Details/192; Liberian Eastern Timber Corp. v. The Government of Liberia, ICSID, 1987. Retrieved January 4, 2025 from https://www.italaw.com/cases/3545; US Department of State Office of the Legal Advisor, Digest of United States Practice in International Law, (2000), at 548. Retrieved January 4, 2025 from https://2009-2017.state.gov/s/l/c8185.htm.

۳. ماده ۲۲ (۳) کنوانسیون روابط دیپلماتیک.

۴. برای بحث در مورد نصب دستگاه‌های شنود توسط دولت پذیرنده در اماکن یک مأموریت دیپلماتیک، به قاعده ۴۱ راهنمای تالین ۲ مراجعه کنید.

5. Tallinn Manual 2.0, op.cit., at 215-216.

6. Virtual Embassies.

می‌گوید، در حالی‌که استونی اعلام کرده یک «سفارت داده»[1] برای پشتیبان‌گیری[2] از داده‌های حیاتی دولتی در سرورهای واقع در کشورهای دوست تأسیس خواهد کرد. با توجه به زمینه‌هایی که ایالات متحده و استونی از اصطلاحات «سفارت مجازی» و «سفارت داده» استفاده کرده‌اند، نگارندگان همچون کارشناسان معتقدند که این نهادها صرفاً به‌دلیل استفاده از واژه «سفارت»، به‌عنوان اماکن یک مأموریت دیپلماتیک شناخته نمی‌شوند.[3] کارشناسان همچنین به این نکته اشاره کردند که برای برقراری روابط دیپلماتیک میان دولت‌ها و به‌ویژه برای تأسیس مأموریت‌های دیپلماتیک دائمی، رضایت متقابل ضروری است.[4] در غیاب چنین رضایتی، «سفارت مجازی» تحت حفاظت ویژه‌ای طبق حقوق دیپلماتیک قرار نمی‌گیرد. باید توجه داشت که اگر زیرساخت‌های سایبری (مانند کامپیوترها، سرورها یا سایر دستگاه‌های شبکه) که یک «سفارت مجازی» یا «سفارت داده» به آن تکیه دارد، در اماکن یک مأموریت دیپلماتیک واقع شده باشد، تحت حفاظت مقرر در این قاعده قرار می‌گیرد. علاوه بر این، داده‌های مربوط به «سفارت مجازی» یا «سفارت داده» که به‌عنوان مکاتبات دیپلماتیک رسمی یا آرشیوها یا اسناد مأموریت دیپلماتیک[5] شناخته می‌شوند همانند آن‌ها تحت حفاظت قرار می‌گیرند.[6]

---

1. Data Embassy.
2. Back Up.

۳. با این حال برای نمونه دولت اتریش بیان داشته است: «زیرساخت‌های فناوری اطلاعات و ارتباطات در محل یک نمایندگی دیپلماتیک یا کنسولی، یک «سفارت داده» یا مقر یک سازمان بین‌المللی از مصونیت برخوردار است». همچنین بیان می‌دارد: «در برخی موارد، زیرساخت‌های فناوری اطلاعات و ارتباطات ممکن است بر اساس معاهدات یا حقوق بین‌الملل عرفی از مصونیت برخوردار باشند. اخیراً برخی کشورها و سازمان‌های بین‌المللی توافق‌نامه‌هایی با سایر کشورها منعقد کرده‌اند که به یک کشور (یعنی کشور فرستنده) یا یک سازمان بین‌المللی اجازه می‌دهد داده‌های خود را در قلمرو کشور دیگری (یعنی کشور پذیرنده) ذخیره یا پردازش کند. لازم به ذکر است که چنین توافق‌نامه‌های دوجانبه تنها برای طرف‌های درگیر الزام‌آور هستند و بر طرف‌های ثالث اثری ندارند. با این حال، فعالیت سایبری که منجر به تخریب داده‌های دولتی در سفارت داده‌ای کشور (الف) در قلمرو کشور (ب) شود، ممکن است به‌عنوان نقض حاکمیت هر دو کشور (الف) و (ب) تلقی گردد».
Position Paper of the Republic of Austria: Cyber Activities and International Law, op.cit., at 14-16.

۴. ماده ۲ کنوانسیون روابط دیپلماتیک.

۵. قاعده ۴۱ راهنمای تالین ۲.

6. Tallinn Manual 2.0, op.cit., at 216.

همچنین کارشناسان به «حضور آنلاین»[1] مأموریت‌های دیپلماتیک توجه کردند. برای نمونه، امروزه برای مأموریت‌های دیپلماتیک معمول است که حساب‌های رسمی در پلتفرم‌های رسانه‌های اجتماعی مانند فیسبوک ایجاد کنند. کارشناسان نتیجه‌گیری کردند که غیرقابل تعرض بودن اماکن یک مأموریت دیپلماتیک به چنین حضور مجازی‌ای اعمال نمی‌شود. برعکس، اماکن یک مأموریت دیپلماتیک به‌طور سنتی به‌معنای حضور فیزیکی در نظر گرفته شده است. در حقیقت، اماکن در ماده ۱ کنوانسیون وین در مورد روابط دیپلماتیک به‌عنوان «ساختمان‌ها یا بخش‌هایی از ساختمان‌ها و زمین‌های مرتبط با آن» تعریف شده‌اند.[2] با این حال مانند «سفارت مجازی» یا «سفارت داده»، کارشناسان اذعان کردند که اگر حضور آنلاین به زیرساخت‌های سایبری که در اماکن فیزیکی یک مأموریت دیپلماتیک واقع شده‌اند وابسته باشد، این زیرساخت‌ها تحت پوشش حفاظت‌های مقرر در این قاعده قرار می‌گیرند. علاوه بر این، آرشیوها، اسناد و مکاتبات رسمی مرتبط با عملیات حضور آنلاین ممکن است در دامنه حفاظتی قواعد ۴۱ و ۴۲ راهنمای تالین ۲ (در ادامه مقاله بررسی می‌شود) قرار گیرند.[3]

۲-۲. وظیفه حفاظت از زیرساخت‌های سایبری

علاوه بر اماکن دیپلماتیک[4]، اسباب و اثاث و اشیاء دیگر موجود در آن و همچنین وسایل نقلیه مأموریت؛ مصون از تفتیش، مصادره، توقیف و یا اجرای احکام قضایی خواهد بود.[5] قاعده ۴۰ راهنمای تالین ۲ بیان می‌دارد: «دولت پذیرنده باید تمام اقدامات مناسب را برای

---

1. Online Presences.

۲. همچنین ماده ۲۱ (۱) کنوانسیون روابط دیپلماتیک.

3. Ibid. at 216-217.

۴. البته اماکنی که از این مصونیت بهره‌مندند، ابنیه‌ای هستند که به‌صورت مؤثر در اختیار مأموریت و برای انجام اشتغالات دیپلماتیک مورد استفاده قرار می‌گیرند و دولت پذیرنده نیز آن‌ها را به‌عنوان اماکن دیپلماتیک پذیرفته، برای آن‌ها قائل به مصونیت شده است. برای مطالعه بیشتر به پرونده زیر رجوع کنید:

Equatorial Guinea v. France, Immunities and Criminal Proceedings Case, ICJ, Merits, Judgment, 2020. Retrieved January 3, 2025 from https://www.icj-cij.org/case/163.

۵. ماده ۲۲ (۳) کنوانسیون روابط دیپلماتیک.

حفاظت از زیرساخت‌های سایبری در اماکن مأموریت دیپلماتیک یا پست کنسولی دولت فرستنده در برابر نفوذ یا آسیب انجام دهد».

بنابراین، دولت پذیرنده «وظیفه‌ای ویژه»[1] دارد که از اماکن مأموریت دیپلماتیک یا پست کنسولی در برابر نفوذ یا آسیب، صرف‌نظر از منبع عملیات موردنظر، محافظت کند.[2] به‌عنوان مثال اگر نیروهای امنیتی دولت پذیرنده متوجه شوند که زیرساخت‌های سایبری دولت فرستنده در داخل اماکن یک مأموریت دیپلماتیک هدف عملیات‌های سایبری قرار گرفته است، دولت پذیرنده باید تمام تلاش‌های معقول را برای خاتمه دادن به این عملیات‌های تخلف‌آمیز از جمله در صورت لزوم، اطلاع‌رسانی به دولت فرستنده در مورد این عملیات‌ها به‌کار گیرد. به همین ترتیب اگر نیروهای امنیتی اطلاع داشته باشند که زیرساخت‌های سایبری مأموریت قرار است هدف عملیات‌های سایبری قرار گیرد، دولت پذیرنده باید اقدامات اجرایی قانون یا سایر تدابیر متناسب و مناسب با تهدید را برای جلوگیری از این عملیات‌ها به‌کار گیرد.[3]

البته تعهد مقرر در این قاعده مطلق نیست. دولت پذیرنده تنها موظف است «تمام اقدامات مناسب»[4] را برای حفاظت از اماکن انجام دهد.[5] به‌طور کلی میزان حفاظت لازم به عواملی همچون بزرگی تهدید برای اماکن، میزان آگاهی دولت پذیرنده از تهدید خاص و ظرفیت دولت پذیرنده برای اقدام در شرایط موجود بستگی دارد. دولت پذیرنده اختیار دارد تا تدابیر خاصی را که برای انجام این وظیفه اتخاذ خواهد کرد، انتخاب کند.[6] با این

---

1. Special Duty.

۲. ماده ۲۲ (۲) کنوانسیون روابط دیپلماتیک؛ ماده ۳۱ (۳) کنوانسیون روابط کنسولی؛

United States of America v. Iran, op.cit., paras. 61–66.

در خصوص اماکن مأموریت دیپلماتیک همچنین مشاهده نمایید؛

Yearbook of the International Law Commission, op.cit., at 78, 95.

با بیان این‌که یک دولت پذیرنده «باید برای انجام این تعهد، تدابیر ویژه‌ای را اتخاذ کند- فراتر از اقداماتی که برای انجام وظیفه عمومی خود برای تضمین نظم انجام می‌دهد».

3. Tallinn Manual 2.0, op.cit., at 217.

4. All Appropriate Steps.

۵. ماده ۲۲ (۲) کنوانسیون روابط دیپلماتیک؛ ماده ۳۱ (۳) کنوانسیون روابط کنسولی.

۶. راهنمای تالین ۲ به پرونده زیر اشاره می‌نماید؛

حال اگرچه حفظ اماکن مأموریت با دولت پذیرنده است، اما در هر صورت ورود به آن‌ها در صورت بروز بحران، نیاز به مجوز رئیس مأموریت دارد. البته عدم صدور این مجوز و به تبع آن عدم مداخله مأموران دولت پذیرنده در سفارتخانه خارجی موجب تبری دولت پذیرنده از مسئولیت در قبال خسارت وارده به آن سفارتخانه نمی‌شود. معهذا به‌نظر می‌رسد در مواردی که خطر جدی برای اشخاص، اموال و سلامت عمومی وجود دارد،[۱] بتوان ورود بدون مجوز مأموران دولت پذیرنده در اماکن مأموریت را مشروع تلقی کرد.[۲]

علاوه بر این، کارشناسان راهنمای تالین ۲ به این نکته توجه کردند که عملیات‌های سایبری که هدفشان اماکن مأموریت‌های دیپلماتیک یا پست‌های کنسولی هستند، اغلب احتمالاً از خارج کشور نشأت می‌گیرند، اما در خصوص این‌که آیا دولت پذیرنده موظف است در صورت لزوم برای حفاظت از اماکن در سرزمین خود از سایر دولت‌ها کمک بخواهد یا نه، به توافقی نرسید. اکثریت بر این عقیده بودند که دولت پذیرنده هیچ تعهدی برای درخواست کمک تحت حقوق دیپلماتیک و کنسولی ندارند؛ وظیفه اتخاذ «اقدامات مناسب» محدود به تدابیری است که شامل استفاده از صلاحیت حاکمیتی آن کشور باشد.

ظاهراً این کارشناسان به عدم وجود رویه‌ای از سوی دولت‌ها که از وجود چنین تعهدی حمایت کند، اشاره کرده‌اند. اقلیت بر این باور بودند که با توجه به منافع مشترک حفظ روابط دیپلماتیک بین دولت‌ها به‌طور کلی، منطقی است که این قاعده به‌گونه‌ای تفسیر شود که شامل تعهدی برای درخواست کمک از سایر دولت‌ها باشد، زمانی‌که چنین کمکی احتمالاً می‌تواند به پایان‌دادن به عملیات‌های سایبری مداخله‌آمیز یا آسیب‌زننده کمک کند.

کارشناسان توافق داشتند که دولت پذیرنده تا زمانی که از یک تهدید خاص آگاه نباشد، هیچ تعهدی برای اتخاذ اقدامات پیشگیرانه برای حفاظت از اماکن مأموریت

Ignatiev v, United States: United States Court of Appeals for the District of Columbia Circuit, Court of Appeals of the United States. 2001. Retrieved January 4, 2025 from https://casetext.com/case/ignatiev-v-us.

۱. برای مثال می‌توان به بروز آتش‌سوزی جدی اشاره کرد.

۲. بیگ‌زاده، پیشین، صص ۸۸۴-۸۸۵.

دیپلماتیک یا پست کنسولی و زیرساخت‌های سایبری موجود در آن ندارد.[۱] در اتخاذ این موضع، کارشناسان به رویه رایج دولت‌های پذیرنده اشاره کردند که معمولاً فقط در صورت وجود خطر امنیتی شناخته‌شده و حتی در آن‌صورت نیز تنها در صورت درخواست رئیس مأموریت یا پست، نیروهای امنیتی ویژه برای حفاظت از اماکن مأموریت یا پست اختصاص می‌دهند.[۲] آن‌ها همچنین خاطرنشان کردند که از نظر عملی، دولت فرستنده احتمالاً برای حفاظت از زیرساخت‌های سایبری موجود در اماکن مأموریت یا پست به تدابیر امنیتی خود، نه به تدابیر امنیتی دولت پذیرنده تکیه خواهد کرد. با این حال، دولت پذیرنده موظف است تمامی اقدامات مناسب را برای «پیشگیری از هرگونه اختلال در آرامش» مأموریت دیپلماتیک یا پست کنسولی و «لطمه به شأن» آن‌ها انجام دهد.[۳]

اگرچه این وظیفه تعریف دقیقی ندارد، کارشناسان توافق داشتند که دولت‌پذیرنده تعهدی برای اقدام علیه صرفاً بیان انتقادات آنلاین از مأموریت دیپلماتیک، پست کنسولی یا دولت فرستنده ندارد. بلکه این تعهد زمانی تحقق می‌یابد که دولت پذیرنده اطمینان حاصل کند که عملکرد واقعی مأموریت یا پست و زیرساخت‌های سایبری موجود در آن مختل نمی‌شود. آن‌ها مشاهده کردند که در عمل، دولت‌ها معمولاً این وظیفه پیشگیرانه را با حقوق بشر در زمینه آزادی بیان و تجمع[۴] متوازن می‌کنند و اگرچه بسیاری از دولت‌ها محدودیت‌هایی بر تجمعات در نزدیکی سفارتخانه‌ها اعمال می‌کنند، معمولاً از ممنوعیت کلی هرگونه سخنرانی در رسانه خاصی که انتقادی از دولت فرستنده یا مأموریت یا پست آن باشد، خودداری می‌کنند.[۵] لذا این قاعده باید در ارتباط با سایر قواعد مندرج در فصل

---

1. Tallinn Manual 2.0, op.cit., at 218.

۲. کارشناسان راهنمای تالین۲ به موارد زیر اشاره می‌نمایند؛

Australian Government, Department of Foreign Affairs and Trade, Protocol Guidelines, para. 12.2, Retrieved January 4, 2025 from https:// www.dfat.gov.au/about-us/publications/corporate/protocol-guidelines; Anthony Minnaar, "Protection of Foreign Missions in South Africa", African Security Review, Vol. 9, No. 2, (2000).

۳. ماده ۲۲ (۲) کنوانسیون روابط دیپلماتیک؛ ماده ۳۱ (۳) کنوانسیون روابط کنسولی.

۴. قاعده ۳۵ راهنمای تالین ۲.

۵. راهنمای تالین ۲ به پرونده‌های زیر اشاره می‌نماید؛

هفتم راهنمای تالین ۲ به‌ویژه قاعده مربوط به تعهد به حفاظت از آزادی ارتباطات یک مأموریت دیپلماتیک یا پست کنسولی[۱] و همچنین قواعد قابل اجرا در سایر بخش‌های این راهنما مانند قواعد مربوط به مراقبت مقتضی[۲] مورد بررسی قرار گیرد.[۳]

۳-۲. مصونیت آرشیوها، اسناد و مکاتبات الکترونیکی

استفاده از پیک به‌عنوان یکی از روش‌های برقراری ارتباطات دیپلماتیک و ارسال مکاتبات و اسناد دارای ماهیت دیپلماتیک و کیسه دیپلماتیک از دیرباز بین کشورها مرسوم بوده است.[۴] حقوق بین‌الملل، مصونیت گسترده‌ای برای آرشیوها، اسناد و مکاتبات رسمی یک مأموریت دیپلماتیک یا پست کنسولی از جمله در قالب الکترونیکی قائل است.[۵] در این راستا در قاعده ۴۱ راهنمای تالین ۲ بیان شده است: «آرشیوها، اسناد و مکاتبات رسمی یک مأموریت دیپلماتیک یا پست کنسولی که به‌صورت الکترونیکی هستند، مصونیت دارند». کارشناسان راهنما توافق داشتند که «مصونیت» به‌معنای آن است که این موارد از ضبط، جاسوسی سایبری[۶]، اجرای قانون یا اقدام قضایی یا هرنوع مداخله دیگر توسط یک دولت

Finzer v. Barry: United States Court of Appeals for the District of Columbia Circuit, Court of Appeals of the United States, 1986. Retrieved January 4, 2025 from https://casetext.com/case/finzer-v-barry; Minister for Foreign Affairs and Trade and others v. Magno and another, Federal Court of Australia, 1992. Retrieved January 4, 2025 from https://ihl-databases.icrc.org/en/national-practice/geraldo-magno-ines-almeida-v-minister-foreign-affairs-and-trade-commissioner.

۱. قاعده ۴۲ راهنمای تالین ۲.

۲. قواعد ۶-۷ راهنمای تالین ۲.

3. Tallinn Manual 2.0, op.cit., at 218-219.

۴. منوچهر توسلی‌نایینی و امیرهمایون قریشی، «وضعیت حقوقی پیک و کیسه دیپلماتیک در حقوق بین‌الملل»، فصلنامه سیاست خارجی، سال ۲۴، شماره ۳، (۱۳۸۹)، ص ۷۷۷.

۵. مواد ۲۴ و ۲۷ (۲) کنوانسیون روابط دیپلماتیک؛ مواد ۳۳ و ۳۵ (۲) کنوانسیون روابط کنسولی؛ همچنین ماده ۶۱ کنوانسیون روابط کنسولی با بیان این‌که: «آرشیو و اسناد پست کنسولی که ریاست آن با مأمور کنسولی افتخاری است در هر زمان و در هر مکان از تعرض مصون خواهد بود، مشروط بر آن‌که از اوراق و اسناد دیگر و مخصوصاً از مکاتبات خصوصی رئیس پست کنسولی و هر شخص دیگری که با او کار می‌کند و همچنین از اموال و کتب و اسناد مربوط به حرفه یا کسب و کار آن‌ها مجزا باشد».

۶. رجوع کنید به قاعده ۳۲ راهنمای تالین ۲.

مصون هستند. هدف از این حفاظت، تضمین محرمانگی است.[۱] البته تنها دولت‌ها ملزم به رعایت این قاعده هستند. اقداماتی که توسط نهادهای خصوصی انجام می‌شوند، تنها در صورتی نقض این قاعده تلقی می‌شوند که به دولت قابل انتساب باشند.[۲]

کارشناسان راهنمای تالین ۲ بر این نظر بودند که «آرشیوها» برای اهداف این قاعده شامل هارددیسک‌های خارجی، فلش درایوها و سایر رسانه‌هایی می‌شود که اسناد الکترونیکی بر روی آن‌ها ذخیره شده‌اند.[۳] اصطلاح «اسناد» نه تنها موارد نهایی به صورت الکترونیکی را دربرمی‌گیرد، بلکه شامل پیش‌نویس‌ها، اسناد مربوط به مذاکرات و سایر موارد مشابهی است که توسط مأموریت‌های دیپلماتیک یا پست‌های کنسولی در جریان فعالیت‌هایشان گردآوری و عمداً حفظ می‌شوند. «مکاتبات رسمی» نیز شامل ایمیل‌ها، دمارش‌ها[۴]، کابل‌ها و سایر پیام‌هایی می‌شود که به یک مأموریت دیپلماتیک، پست کنسولی یا وظایف آن‌ها مربوط می‌شود.[۵]

کارشناسان درباره این‌که آیا ارسال‌های خصوصی به یک مأموریت یا پست از طریق ایمیل یا حضور آنلاین به‌عنوان آرشیوها، اسناد یا مکاتبات رسمی تحت حمایت این قاعده محسوب می‌شوند یا نه؟ دچار اختلاف‌نظر بودند. برای مثال ممکن است وب‌سایت یک مأموریت دیپلماتیک یا پست کنسولی به شهروندان دولت پذیرنده اجازه دهد درخواست‌های آنلاین برای ویزا جهت سفر به دولت فرستنده ارائه دهند. اکثریت کارشناسان بر این باور بودند که گسترش حمایت از این موارد با موضوع و هدف قواعد دیپلماتیک و کنسولی سازگار است و این‌که اطلاعاتی که به‌طور رسمی ارسال می‌شود حداقل به‌عنوان بخشی از آرشیوها و اسناد مأموریت یا پست در نظر گرفته می‌شود. تعداد

---

1. Tallinn Manual 2.0, op.cit, at 219.

۲. قواعد ۱۵ و ۱۷ راهنمای تالین ۲.

۳ هم‌چنین مشاهده نمایید ماده ۱ (۱) (ک) کنوانسیون روابط کنسولی در خصوص «آرشیوهای کنسولی» که بیان می‌دارد: «اصطلاح «آرشیو کنسولی» شامل کلیه اوراق و اسناد و مکاتبات و کتاب‌ها و فیلم‌ها و نوارهای ضبط صوت و دفاتر پست کنسولی به انضمام رمز و مفتاح و کارت‌های اندکس و هر نوع اثاثه که برای حفاظت و نگهداری آن‌ها به‌کار برده شود – خواهد بود».

4. Demarches.

5. Ibid., at 220.

کمی از کارشناسان دیدگاه مخالف داشتند و معتقد بودند که چنین ارسال‌های خصوصی خارج از محدوده این قاعده قرار می‌گیرند، زیرا قواعد دیپلماتیک و کنسولی محدود به روابط بین دولت‌ها هستند. با این حال، تمامی کارشناسان توافق داشتند که اگر برای مثال یک شهروند دولت پذیرنده نظری را زیر آخرین پست مأموریت در یک وب‌سایت رسانه اجتماعی منتشر کند، آن نظر تحت حمایت این قاعده نخواهد بود، زیرا عمومی است و در دسترس همگان قرار دارد.[۱]

علاوه بر آرشیوهای الکترونیکی، اسناد و مکاتبات رسمی مأموریت دیپلماتیک که به‌صراحت در این قاعده ذکر شده‌اند، مصونیت شامل مکاتبات و اسناد شخصی مأموران دیپلماتیک نیز می‌شود.[۲] استفاده از پیک به‌عنوان یکی از روش‌های برقراری ارتباطات دیپلماتیک و ارسال مکاتبات و اسناد دارای ماهیت دیپلماتیک و کیسه دیپلماتیک از دیرباز بین کشورها مرسوم بوده است. با این حال، مصونیت شامل مکاتبات و اسناد شخصی مأموران کنسولی یا کارکنان یک پست کنسولی نمی‌شود.[۳]

مصونیت آرشیوها و اسناد مأموریت دیپلماتیک یا پست کنسولی، طبق نظر کارشناسان راهنمای تالین ۲، «در هر زمان و هر مکانی که باشند»[۴] برقرار است. بنابراین، آرشیوها و اسناد الکترونیکی مأموریت یا پست حتی زمانی که خارج از قلمرو دولت پذیرنده باشند، مصونیت خود را حفظ می‌کنند. برای نمونه اگر آرشیوهای مأموریت دیپلماتیک روی سِرور دولتی در خارج از قلمرو دولت پذیرنده مانند سرور وزارت امور خارجه دولت ارسال‌کننده ذخیره شده باشند، همچنان مصونیت دارند. به همین ترتیب اگر اسناد روی زیرساخت‌های خصوصی سایبری مانند سرور ایمیل خصوصی یا زیرساخت ابری خصوصی[۵] ذخیره شده باشند، تا زمانی که دولت ارسال‌کننده قصد دارد این موارد را

---

1. Ibid.

۲. ماده ۳۰ (۲) کنوانسیون روابط دیپلماتیک.

۳. این نتیجه‌گیری همچنین با این واقعیت تأیید می‌شود که هیچ ماده قابل مقایسه با ماده ۳۰ (۲) کنوانسیون وین در مورد روابط دیپلماتیک در کنوانسیون وین در مورد روابط کنسولی وجود ندارد.

۴. ماده ۲۴ کنوانسیون روابط دیپلماتیک؛ ماده ۳۳ کنوانسیون روابط کنسولی.

5. Private Cloud Infrastructure.

محرمانه نگه دارد و آن‌ها را با رضایت خود به طرف ثالثی افشا نکرده باشد[۱]، این اسناد مصونیت خواهند داشت.[۲]

کارشناسان توافق کردند که حقوق معاهداتی و عرفی، تمامی دولت‌ها – و نه فقط دولت پذیرنده – را موظف می‌کند که مکاتبات رسمی دیپلماتیک و کنسولی و دیگر ارتباطات رسمی «در حال انتقال» را همانند آزادی و حمایتی که دولت پذیرنده ملزم به ارائه آن است، رعایت و حمایت کنند.[۳] بنابراین، کارشناسان این دادگاه را پذیرفتند که هر دو دولت پذیرنده و دولت‌های ثالث از رهگیری ارتباطات الکترونیکی مأموریت‌های دیپلماتیک و پست‌های کنسولی که در حال انتقال هستند، ممنوع می‌باشند. در این راستا کارشناسان تأکید کردند که محرمانگی ارتباطات دیپلماتیک و کنسولی برای انجام وظایف مأموریت دیپلماتیک یا پست کنسولی امری ضروری و بنیادی است اما کارشناسان درباره این پرسش اختلاف‌نظر داشتند که آیا همه دولت‌ها و نه صرفاً دولت پذیرنده موظفند مصونیت از تعرض اسناد و مواد دیپلماتیک و کنسولی دولت فرستنده را در زمانی که این اسناد و مواد در حالت ثابت (در محل نگهداری) قرار دارند و نه در حال انتقال (ترانزیت)، رعایت کنند یا نه.

آن‌ها اشاره کردند زمانی که این موارد در داخل اماکن یک هیأت دیپلماتیک یا پست کنسولی ذخیره می‌شود، ممکن است تحت مصونیت اماکن قرار گیرد.[۴] اما زمانی‌که این موارد خارج از هیأت یا پست قرار دارند مانند داده‌هایی که در یک سرور ابری خصوصی ذخیره شده‌اند، کارشناسان اختلاف‌نظر داشتند. اقلیتی از آن‌ها بر این باور بودند که تعمیم این تعهد به دولت‌های ثالث با موضوع و هدف اصل مصونیت سازگار است، به‌ویژه با توجه به سهولتی که دولت‌ها اکنون می‌توانند به داده‌های الکترونیکی خارج از قلمرو خود

---

۱. بر اساس قاعده ۱۹ راهنمای تالین ۲.

2. Tallinn Manual 2.0, op.cit., at 221.

۳. اشخاص ثالث نیز ملزم به رعایت مصونیت سایر دسته‌های موارد دیپلماتیک و کنسولی در ترانزیت مانند کیسه دیپلماتیک یا کنسولی هستند (مواد ۴۰ (۳) کنوانسیون روابط دیپلماتیک و مواد ۵۴ (۳) کنوانسیون روابط کنسولی)؛ همچنین برای مطالعه بیشتر رجوع نمایید به پیش‌نویس مواد راجع به وضعیت پیک دیپلماتیک و کیسه دیپلماتیک که همراه پیک دیپلماتیک نمی‌باشد و پیش‌نویس پروتکل‌های اختیاری ۱۹۸۹.

۴. به بحث‌های پیشین درخصوص قاعده ۳۹ راهنمای تالین ۲ مراجعه کنید.

دسترسی پیدا کنند. اما اکثریت کارشناسان دیدگاه مخالفی اتخاذ کردند و بر این اساس اظهار داشتند که تعهدات خاصی که در متون معاهدات مربوط به دولت‌های ثالث تحمیل شده است، به‌طور صریح به مصونیت مکاتبات رسمی و سایر ارتباطات در حال عبور محدود شده و بنابراین به موارد دیپلماتیک یا کنسولی که در وضعیت استقرار هستند، تسری نمی‌یابد.[1]

علاوه بر این، کارشناسان درباره دامنه دقیق ممنوعیت نظارت الکترونیکی دولت‌های ثالث بر ارتباطات دیپلماتیک اختلاف‌نظر داشتند. به‌ویژه آن‌ها بر سر این موضوع اختلاف داشتند که آیا موارد محافظت‌شده از رهگیری توسط دولت ثالث، محدود به ارتباطات بین هیأت دیپلماتیک و دولت فرستنده است یا شامل ارتباطات بین دولت فرستنده و دولت پذیرنده؟ و همچنین بین هیأت دولت فرستنده و هیأت‌های سایر دولت‌ها در دولت پذیرنده نیز می‌شود.

اکثریت کارشناسان بر این نظر بودند که این ممنوعیت به تمامی چنین مکاتباتی تسری می‌یابد و در تأیید این دیدگاه به مصونیت عام از تعرض که مکاتبات رسمی به طور کلی از آن برخوردارند، این واقعیت که چنین مکاتباتی در قلمرو «تمامی مکاتبات مربوط به مأموریت و وظایف آن» قرار می‌گیرند و نیز به سوابق مذاکراتی کنوانسیون وین درباره روابط دیپلماتیک استناد کردند؛ سوابقی که نشان می‌دهد اصل آزادی ارتباطات قرار نبوده است که صرفاً به ارتباط میان مأموریت دیپلماتیک و دولت فرستنده آن محدود شود، بلکه مقصود آن بوده است که تمامی مکاتبات رسمی را دربر گیرد از جمله ارتباط میان مأموریت دیپلماتیک یک دولت فرستنده با دولت پذیرنده یا با مأموریت‌های دیپلماتیک سایر دولت‌ها.[2]

به‌عبارت دیگر اکثریت نتیجه گرفتند که حقوق دیپلماتیک عموماً به‌منظور تقویت محرمانگی ارتباطات دیپلماتیک وضع شده است و دلیلی برای ایجاد استثناء در این دسته از ارتباطات وجود ندارد. عده‌ای از کارشناسان معتقد بودند که این ممنوعیت، تنها ارتباطات هیأت دیپلماتیک با دولت فرستنده خود را در بر می‌گیرد. آن‌ها به نبود زبان

1. Tallinn Manual 2.0, op.cit., at 221-222.
2. Yearbook of the International Law Commission, op.cit., at 137–138.

صریح در ممنوعیت رهگیری سایر انواع ارتباطات اشاره کرده و تأکید داشتند که یکی از موضوعات و هدف بنیادین حقوق دیپلماتیک، تضمین توانایی مأموریت در برقراری ارتباط ایمن با دولت خود است.[۱]

همچنین کارشناسان اشاره کردند که به‌نظر می‌رسد دولت‌ها به‌طور مکرر ممنوعیت‌های پیش‌گفته را با گزارش‌های متعدد از نظارت دولت‌های پذیرنده بر ارتباطات دیپلماتیک دولت‌های فرستنده و قرار دادن دستگاه‌های شنود در مأموریت‌های دیپلماتیک دولت‌های فرستنده نقض کرده‌اند. با این حال، کارشناسان مشاهده کردند که در این موارد، دولت‌های فرستنده همچنان نظارت را به‌عنوان نقض حقوق بین‌الملل مورد اعتراض قرار می‌دهند؛ محکومیت این اقدامات معمولاً توسط دولت‌های متهم به چنین فعالیت‌هایی، حداقل بر مبنای حقوق بین‌الملل بی‌پاسخ می‌ماند.[۲] به همین‌دلیل کارشناسان نتیجه گرفتند که باور حقوقی[۳] به نفع قانونی دانستن چنین نظارتی شکل نگرفته است. به‌عبارت دیگر، ممنوعیت موجود در حقوق بین‌الملل در خصوص نظارت بر مطالب دیپلماتیک همچنان به قوت خود باقی است.[۴]

لازم به ذکر است مواردی که مورد اشاره قرار گرفته‌اند به‌صورت نامحدود تحت حفاظت قرار دارند. این امر حتی در صورت بسته شدن مأموریت، قطع روابط دیپلماتیک یا وقوع مخاصمه مسلحانه[۵] نیز صادق است. در واقع کنوانسیون وین، هم درباره روابط

---

1. Tallinn Manual 2.0, op.cit., at 222-223.

۲. کارشناسان راهنمای تالین ۲ به موارد زیر اشاره می‌نمایند؛

Reuters, China demands U.S. explain spying allegations linked to Australian missions, 2013. Retrieved January 4, 2025 from https:// www. reuters. com/ article/ world/china-demands-u-s-explain-spying-allegations-linked-to-australian-missions-idUSBRE99U0LU/; Spiegel, Et Tu, UK? Anger Grows over British Spying in Berlin, 2013. Retrieved January 4, 2025 from https:// www. spiegel.de/ international/ europe/revelation-of-spy-nest-in-british-berlin-embassy-angers-germans-a-931868.html; Kuwait News Agency, MI5 Tried to Bug London Embassy, says Pakistan, 2003. Retrieved January 4, 2025 from https:// www. kuna. net.kw/ Article Details. aspx?id=1404317&language=en.

3. Opinio Juris.

4. Tallinn Manual 2.0, op.cit, at 223; Nicaragua v. United States of America, Military and Paramilitary Activities in and against Nicaragua, ICJ, Judgment, 1986, para 186. Retrieved January 9, 2025 from https://www.icj-cij.org/case/70.

۵. مطابق قواعد ۸۲–۸۳ راهنمای تالین ۲.

دیپلماتیک و هم درباره روابط کنسولی، دولت پذیرنده را ملزم می‌کنند که پس از قطع روابط یا فراخوان کارکنان مأموریت یا پست کنسولی، «به اموال و آرشیوهای مأموریت احترام گذاشته و از آن‌ها حفاظت کند».[۱]

همچنین کارشناسان راهنمای تالین ۲ بر این باور بودند که مصونیت آرشیوها، اسناد و مکاتبات رسمی یک مأموریت دیپلماتیک یا پست کنسولی حتی در صورتی‌که این موارد به‌صورت غیرقانونی سرقت یا توسط شخص ثالث (ازجمله یک دولت دیگر) به‌دست آید و سپس به دولتی که ملزم به رعایت مصونیت آن است ارائه شود یا به هر نحو در اختیار آن قرار گیرد، هم‌چنان پابرجا است. بنابراین، دولت‌ها نمی‌توانند با بهره‌گیری از یک واسطه که در ابتدا این موارد حفاظت‌شده را به‌دست آورده است، از تعهد خود به رعایت مصونیت موارد دیپلماتیک یا کنسولی شانه خالی کنند.[۲]

در خصوص این پرسش که آیا مصونیت در صورت دستیابی شخص ثالث (از جمله یک دولت دیگر) به موارد دیپلماتیک یا کنسولی و سپس در دسترس قرار دادن آن‌ها برای عموم مردم پابرجا می‌ماند، کارشناسان اختلاف‌نظر داشتند. برای نمونه، این موارد ممکن است به سرقت رفته یا به‌صورت غیرقانونی به‌دست آمده و سپس در اینترنت منتشر شوند مانند آن‌چه در حادثه ویکی‌لیکس[۳] رخ داد. اکثریت کارشناسان معتقد بودند که این قاعده دیگر قابل اعمال نیست، زیرا موضوع و هدف آن که حفظ محرمانگی این موارد است، نقض شده است. به‌عبارت دیگر اگر این موارد به‌طور علنی در دسترس باشند، از لحاظ عملی محرمانه محسوب نمی‌شوند.[۴] با این حال، نگارندگان هم‌نظر با اقلیتی از کارشناسان

---

۱. ماده ۴۵ کنوانسیون روابط دیپلماتیک؛ ماده ۲۷ (الف) کنوانسیون روابط کنسولی.

۲. کارشناسان تأکید کردند که قواعد انتساب در حقوق مسئولیت بین‌المللی دولت‌ها (مطابق قواعد ۱۵–۱۸ راهنمای تالین ۲) در این موضوع قابل اعمال است.

Tallinn Manual 2.0, op.cit., at 223.

3. Wikileaks.

۴. راهنمای تالین ۲ به پرونده زیر اشاره می‌نماید؛

R (Bancoult) v. Secretary of State for Foreign and Commonwealth Affairs, Court of Appeal of United Kingdom, Judgment, 2014, para 58. Retrieved January 4, 2025 from https://vlex.co.uk/vid/r-on-the-application-793368225.

بر این باور هستند که این قاعده حتی در چنین مواردی نیز همچنان قابل اجرا است. این کارشناسان تأکید داشتند که ادامه احترام به مصونیت، تا جایی‌که در شرایط ممکن باشد، احتمالا به بازگرداندن ماهیت محرمانه موارد کمک کند یا از استنباط‌هایی که ممکن است به ضرر دولت ارسال‌کننده یا دیپلمات‌های آن باشد، جلوگیری نماید. علاوه بر این، دولت ارسال‌کننده ممکن است تمایل داشته باشد مصونیت این موارد را نسبت به دولت‌هایی که هنوز به اطلاعات دسترسی پیدا نکرده‌اند حفظ کند و هم‌زمان اقدامات قانونی علیه افرادی که این موارد به‌دست آن‌ها افتاده است، انجام دهد. در نهایت، این کارشناسان به گستردگی هنجار مصونیت و اهمیت مرکزی آن در روابط دیپلماتیک اشاره کرده و بنابراین، دامنه حفاظتی «هرکجا که باشند»[۱] را شامل حوزه عمومی نیز تفسیر کردند.[۲]

از طرف دیگر، دولت‌ها به‌طور فزاینده‌ای از حضور آنلاین برای انجام برخی از وظایف دیپلماتیک و کنسولی خود مانند ارائه اطلاعات در مورد وضعیت امنیتی دولت پذیرنده برای شهروندان خود در دولت پذیرنده استفاده می‌کنند. در این رابطه، کارشناسان راهنمای تالین ۲ به این نتیجه رسید که اطلاعات یا مواردی که به‌صورت عمومی توسط دولت ارسال‌کننده در دسترس قرار می‌گیرد، مشمول حمایت این قاعده نیست؛ زیرا موضوع و هدف اصلی این قاعده تضمین محرمانگی موارد دیپلماتیک و کنسولی است. به‌عنوان مثال اگر یک دولت وب‌سایت مأموریت دیپلماتیک دولت دیگر را تخریب کند، این قاعده نقض نمی‌شود، اگرچه چنین اقدامی ممکن است قاعده دیگری که در فصل هفتم راهنما مقرر شده است مانند مصونیت زیرساخت سایبری در محل‌های دیپلماتیک[۳] را نقض کند.[۴]

به‌علاوه کارشناسان توافق داشتند که در حال حاضر در حقوق بین‌الملل عرفی هیچ الزامی وجود ندارد که آرشیوها، اسناد یا مکاتبات رسمی الکترونیکی یک مأموریت دیپلماتیک یا پست کنسولی برای برخورداری از مصونیت، باید به‌طور خاص

(با یافتن این نکته، تشخیص اینکه یک تلگرام دیپلماتیک که حاوی مکاتبات دیپلماتیک بوده و به مطبوعات درز کرده است، به‌عنوان دلیل قابل پذیرش در دادگاه محسوب می‌شود).

۱. ماده ۲۴ کنوانسیون روابط دیپلماتیک؛ ماده ۳۳ کنوانسیون روابط کنسولی.

2. Tallinn Manual 2.0, op.cit., at 224.

۳. قاعده ۳۹ راهنمای تالین ۲.

4. Ibid. at 224.

علامت‌گذاری شوند. کارشناسان به فقدان رویه دولتی در این زمینه اشاره کردند و همچنین تاریخچه مذاکرات کنوانسیون وین درباره روابط دیپلماتیک را یادآور شدند[1] که در آن پیشنهادهایی برای اعمال چنین شرطی بر آرشیوهای فیزیکی رد شده بود.[2]

در نهایت کارشناسان به استفاده فزاینده از کنسول‌های افتخاری توجه کردند. برای تشویق روابط اقتصادی و در عین حال کاهش هزینه‌های تأسیس پست‌های کنسولی، بسیاری از دولت‌ها از بازرگانان یا سایر حرفه‌ای‌ها برای ایفای نقش به‌عنوان نمایندگان کنسولی به‌صورت نیمه‌وقت استفاده می‌کنند.[3] هرچند اسناد، مکاتبات و آرشیوهای یک پست کنسولی که توسط یک کنسول افتخاری اداره می‌شود مصونیت دارند، این مصونیت مشروط بر این است که این موارد از مواردی که به سایر فعالیت‌های حرفه‌ای کنسول افتخاری مربوط می‌شوند، جدا نگه داشته شوند.[4]

۴-۲. آزادی ارتباطات

اینترنت عمدتاً به‌عنوان وسیله‌ای برای ارتباطات استفاده می‌شود. از این‌رو ارتباط نزدیکی با آزادی ارتباطات در دیپلماسی دارد؛[5] لذا یکی از مهم‌ترین آزادی‌ها برای یک مأموریت سیاسی و کنسولی، آزادی ارتباطات رسمی آن مأموریت با دولت فرستنده یا دیگر نمایندگی‌های آن دولت است. یکی از ارکان این آزادی، استفاده از پیک برای فرستادن مکاتبات و اسناد دارای ماهیت دیپلماتیک و کیسه دیپلماتیک بوده است.[6] از این‌رو در

---

1 United Nations Conference on Diplomatic Intercourse and Immunities, United States of America: amendment to article 22 (A/CONF.20/C.1/L.153), (1961). Retrieved January 4, 2025 from https:// legal. un. org/ diplomaticconferences/ 1961_dipl_intercourse/docs/english/vol_2.pdf; United Nations Conference on Diplomatic Intercourse and Immunities, Official Records (A/CONF.20/14), (1961), at 149. Retrieved January 4, 2025 from https:// documents. un.org/ doc/ undoc/ gen/ g62/016/03/pdf/g6201603.pdf.

2. Tallinn Manual 2.0, op.cit., at 225.

3. Ibid.

۴. ماده ۶۱ کنوانسیون روابط کنسولی.

5. Choi, op.cit., at 224.

۶. منوچهر توسلی نایینی، «آزادی ارتباطات مأموریت‌های دیپلماتیک در حقوق بین‌الملل و جایگاه حقوقی پیک و کیسه دیپلماتیک در آن» ، فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی، دوره ۱۹، شماره ۷۳، (۱۳۹۵)، صص ۱۹۹-۲۲۶.

حقوق بین‌الملل معاهداتی تصریح شده است که دولت پذیرنده باید آزادی ارتباطات مأموریت دیپلماتیک یا پست کنسولی دولت فرستنده را برای همه مقاصد رسمی مجاز بداند و از آن محافظت کند.[۱] در خصوص پست‌های کنسولی، قابل توجه است که حق مأموران کنسولی برای آزادی ارتباطات با اتباع دولت فرستنده به‌رسمیت شناخته شده است.[۲] بنابراین دولت‌پذیرنده نمی‌تواند برای مثال در ارتباطات ایمیلی بین مأموران کنسولی و اتباع دولت فرستنده در رابطه با امور رسمی کنسولی مداخله کند.[۳] کارشناسان راهنمای تالین ۲ توافق داشتند که این مقرره بازتابی از حقوق بین‌الملل عرفی است.[۴] در این راستا قاعده ۴۲ راهنمای تالین ۲ بیان می‌دارد: «دولت پذیرنده موظف است آزادی ارتباطات سایبری یک مأموریت دیپلماتیک یا پست کنسولی را برای همه مقاصد رسمی اجازه داده و از آن محافظت کند».

کارشناسان راهنمای تالین ۲ اشاره کردند که کنوانسیون وین درباره روابط کنسولی از عبارت «اجازه دادن و محافظت از آزادی ارتباطات»[۵] به‌جای «آزادی ارتباطات»[۶] استفاده کرده است که به‌طور واضح‌تر موضوع و هدف این مقرره را بیان می‌کند. از نظر کارشناسان، اصطلاح «اجازه دادن»[۷] و ارجاع به «آزادی»[۸] به این معنا است که دولت‌های پذیرنده نمی‌توانند توانایی یک مأموریت دیپلماتیک یا پست کنسولی برای ارتباط از طریق روش‌های سایبری یا الکترونیکی دیگر را مختل کنند. برای مثال دولت پذیرنده نمی‌تواند دسترسی به وب‌سایت مأموریت دیپلماتیک یا پست کنسولی که برای ارائه اطلاعات ضروری به اتباع آن در کشور استفاده می‌شود را مختل کند، اتصال اینترنتی مأموریت دیپلماتیک یا پست کنسولی را قطع یا کند نماید یا تجهیزات تلفن همراه یا سایر وسایل

---

۱. ماده ۲۷ (۱) کنوانسیون روابط دیپلماتیک؛ ماده ۳۵ (۱) کنوانسیون روابط کنسولی.

۲. ماده ۳۶ (۱) (الف) کنوانسیون روابط کنسولی.

3. Tallinn Manual 2.0, op.cit., at 225-226.
4. Ibid. at 225.
5. Permit and Protect Freedom of Communication.
6. Freedom Communication.
7. Permit.
8. Freedom.

ارتباطی آن‌ها را مسدود یا مختل کند. اصطلاح «اجازه دادن» به‌معنای این نیست که دولت فرستنده باید برای برقراری ارتباطات سایبری از دولت پذیرنده مجوز بگیرد.[۱]

علاوه بر این، تعهدات دولت پذیرنده صرفاً به اجازه دادن به آزادی ارتباطات سایبری یک مأموریت دیپلماتیک یا پست کنسولی محدود نمی‌شود. دولت پذیرنده همچنین موظف است برای «حفاظت»[۲] از ارتباطات آن‌ها در برابر اختلال دیگران اقدام کند. کارشناسان بر این باور بودند همان استانداردی که برای وظیفه حفاظت از زیرساخت سایبری در محل مأموریت یا پست[۳] اعمال می‌شود، به حفاظت از ارتباطات سایبری آزاد نیز تسری دارد؛ یعنی دولت پذیرنده باید «تمام اقدامات مناسب» را برای اطمینان از این حفاظت انجام دهد. مشابه حفاظت از زیرساخت سایبری، این تعهد مطلق نیست. تعهد خاص با توجه به میزان خطر و تهدیداتی که ارتباطات سایبری را تهدید می‌کنند، متناسب است.

بر اساس وظیفه حفاظت، کارشناسان توافق داشتند که برای نمونه اگر مقامات دولت پذیرنده از طریق دولت فرستنده یا هر منبع دیگری مطلع شوند که ارتباطات سایبری دولت فرستنده دچار اختلال شده است، باید اقدامات مناسب برای رفع این اختلال را انجام دهند. آن‌ها همچنین توافق کردند که دولت پذیرنده موظف است اقداماتی برای متوقف کردن رهگیری ارتباطات سایبری دیپلماتیک از جمله توسط سایر دولت‌ها[۴] که در قلمرو آن انجام می‌شود،[۵] اتخاذ کند.[۶]

---

1. Tallinn Manual 2.0, op.cit., at 226.
2. Protect.

۳. مطابق قاعده ۴۰ راهنمای تالین ۲.

۴. مطابق قاعده ۴۱ راهنمای تالین ۲.

۵. ارتباطات سایبری چالش‌های ویژه‌ای را در رابطه با تعهد به حفاظت به همراه دارد. به‌عنوان نمونه، در پرونده‌ای مربوط به سال ۲۰۰۲، افراد ناشناسی ایمیل‌های سیاسی حساس ارسال‌شده توسط سفیر اتحادیه اروپا در ترکیه را رهگیری کرده و سپس این ایمیل‌ها را با یک مجله ترک به اشتراک گذاشته و منتشر کردند. دولت ترکیه وعده داد که این حادثه را مورد تحقیق قرار داده و عاملان آن را تحت پیگرد قرار دهد و پس از چند روز انتشار بیشتر این ایمیل‌ها را ممنوع کرد، اما هم‌چنین اذعان داشت که نظارت بر اینترنت یک مشکل گسترده است که هیچ دولتی تاکنون نتوانسته است پاسخ مؤثری برای آن ارائه دهد.

Tallinn Manual 2.0, op.cit., at 226.

6. Ibid. at 226.

همچنین کارشناسان تأکید کردند که تعهدات دولت پذیرنده برای «اجازه دادن» و «حفاظت کردن» محدود به ارتباطات سایبری «رسمی» است. به‌عنوان مثال اگر هکرهایی در دولت پذیرنده وب‌سایت رسمی یک هیأت یا نمایندگی را هدف قرار دهند، دولت پذیرنده باید اقداماتی که به‌طور معقول در دسترس است را برای متوقف کردن این فعالیت‌ها انجام دهد. با این حال، دولت پذیرنده موظف نیست امکان برقراری ارتباطات شخصی نمایندگان دیپلماتیک را مانند استفاده از حساب‌های ایمیل شخصی مجاز بداند یا از آن‌ها حفاظت کند. کارشناسان اذعان داشتند که گاهی تمایز بین وظایف رسمی و غیررسمی دشوار است. این مسئله به‌ویژه در رابطه با دیپلماسی عمومی که خطاب به جمعیت دولت پذیرنده است، مطرح می‌شود. در نبود باور حقوقی در این حوزه، کارشناسان نتوانستند به نتیجه قطعی در این زمینه دست یابند.[1]

از سوی دیگر، کارشناسان بررسی کردند که آیا دولت پذیرنده با منع یک هیأت دیپلماتیک از ایجاد و بهره‌برداری از حضور آنلاین مانند یک وب‌سایت یا حساب کاربری در شبکه‌های اجتماعی، به این قاعده تخطی می‌کند یا نه؟ به این دلیل که امور رسمی با دولت پذیرنده باید با یا از طریق وزارت امور خارجه یا وزارت دیگری که مورد توافق قرار گرفته است، مطابق با ماده ۴۱ (۲)[2] کنوانسیون وین در خصوص روابط دیپلماتیک، انجام شود. کارشناسان توافق کردند که الزام مندرج در ماده ۴۱ (۲) صرفاً برای روشن‌کردن این است که چه نهادی در دولت‌پذیرنده باید نقطه تماس رسمی اصلی برای امور رسمی بین دولت‌های فرستنده و پذیرنده باشد. کارشناسان خاطرنشان کردند که بسیاری از امور رسمی دیپلماتیک که توسط نمایندگان خارجی در دولت‌های پذیرنده انجام می‌شود، خارج از این کانال‌های رسمی صورت می‌گیرد؛ همچنین این موضوع را متذکر شدند که معمولاً سفرای کشورها و دیگر نمایندگان دیپلماتیک، سخنرانی‌هایی برای مخاطبان خصوصی ارائه می‌دهند، میزگردهایی برگزار می‌کنند و به‌طور رسمی با

---

1. Ibid. at 227.

۲. ماده ۴۱ (۲) کنوانسیون روابط دیپلماتیک بیان می‌دارد: «کلیه امور رسمی که برای اقدام و مذاکره با کشور پذیرنده از طرف کشور فرستنده به عهده مأموریت گذاشته شده باید از طریق وزارت امور خارجه کشور پذیرنده یا به‌وسیله آن و یا هر وزارتخانه دیگری که مقرر است انجام گیرد».

اشخاص خصوصی در دولت پذیرنده تعامل دارند و این‌که این روش‌ها به‌عنوان روش‌های پذیرفته‌شده برای انجام وظایف دیپلماتیک از جمله نمایندگی دولت فرستنده، ارزیابی شرایط و تحولات در دولت پذیرنده و ترویج روابط دوستانه میان دولت‌های فرستنده و پذیرنده شناخته می‌شوند.[۱]

۵-۲. استفاده از اماکن و فعالیت‌های رسمی

اماکن یک هیأت دیپلماتیک نباید به‌نحوی مورد استفاده قرار گیرند که با وظایف یک هیأت دیپلماتیک ناسازگار باشد.[۲ و ۳] به‌طور مشابه، پست‌های کنسولی نیز نباید به‌نحوی مورد استفاده قرار گیرند که با وظایف کنسولی ناسازگار باشند.[۴ و ۵] بنابراین، برای نمونه،

---

1. Ibid. at 227.

۲. ماده ۴۱ (۳) کنوانسیون روابط دیپلماتیک.

۳. مطابق ماده ۳ کنوانسیون روابط دیپلماتیک، این وظایف شامل موارد زیر اما نه محدود به آنها است:

الف- بازنمایی «نمایندگی» دولت فرستنده نزد دولت‌پذیرنده؛

ب- حفاظت از منافع دولت فرستنده و اتباع آن در دولت پذیرنده، در حدود مجاز توسط حقوق بین‌الملل؛

پ- مذاکره با حکومت دولت پذیرنده؛

ت- کسب اطلاع از اوضاع و احوال و تحول وقایع در دولت پذیرنده با تمام وسایل قانونی و گزارش‌دهی به دولت فرستنده و

ث- ترویج روابط دوستانه بین دولت‌فرستنده و دولت‌پذیرنده و توسعه روابط اقتصادی، فرهنگی و علمی.

۴. ماده ۵۵ (۲) کنوانسیون روابط کنسولی.

۵. مطابق ماده ۵ کنوانسیون روابط کنسولی، وظایف کنسولی مرتبط با فعالیت‌های سایبری شامل موارد زیر اما نه محدود به آنها است:

الف- حمایت از منافع دولت فرستنده و اتباع آن (اعم از اشخاص حقیقی و حقوقی) در دولت پذیرنده با رعایت محدوده‌های پذیرفته‌شده در حقوق بین‌الملل؛

ب- تسهیل و توسعه روابط تجاری، اقتصادی، فرهنگی و علمی میان دولت فرستنده و دولت پذیرنده و ارتقای روابط دوستانه به هر طریق دیگر میان آن‌ها در چارچوب مقررات کنوانسیون حاضر؛

پ- کسب اطلاع از اوضاع و احوال و تحول وضعیت تجاری، اقتصادی، فرهنگی و علمی دولت پذیرنده با استفاده از وسایل مجاز و گزارش آن به حکومت دولت فرستنده و ارائه اطلاعات به اشخاص ذی‌نفع؛

ت- صدور گذرنامه و مدارک سفر برای اتباع دولت فرستنده و همچنین صدور روادید (ویزا) و اسناد لازم به اشخاصی که قصد ورود به آن دولت را دارند؛

ث- ارائه کمک و هم‌یاری به اتباع (اعم از اشخاص حقیقی و حقوقی) دولت فرستنده؛

جمع‌آوری اطلاعات تا زمانی که به شیوه‌ای مطابق با قوانین داخلی دولت پذیرنده انجام شود، مشروع است. در مقابل، اکثر دولت‌ها، جاسوسی از جمله جاسوسی اقتصادی را طبق قوانین داخلی خود جرم‌انگاری می‌کنند[1] و بنابراین رفتاری که تحت چنین ممنوعیت‌های داخلی قرار می‌گیرد، نقض ماده ۴۱ کنوانسیون روابط دیپلماتیک نیز خواهد بود.

در این راستا قاعده ۴۳ راهنمای تالین ۲ بیان می‌دارد: «الف- اماکن یک هیأت دیپلماتیک یا پست کنسولی نباید برای انجام فعالیت‌های سایبری که با وظایف دیپلماتیک

ج- انجام وظیه در مقام مامور ثبت احوال و انجام اشتغالات مشابه و همچنین برخی اشتغالات اداری تا آن‌جا که مغایر با قوانین و مقررات دولت پذیرنده نباشد؛

چ- حفظ منافع اتباع (اعم از حقیقی و حقوقی) دولت فرستنده در مورد مسائل مرتبط با وراثت در دولت پذیرنده طبق قوانین و مقررات این دولت؛

ح- حفظ منافع اتباع صغیر و محجور دولت فرستنده در دولت پذیرنده در حدود پیش‌بینی شده در قوانین و مقررات این دولت به‌ویژه زمانی که وجود قیم یا ولی برای آن افراد ضروری است؛

خ- با رعایت عملکرد و روند جاری در دولت پذیرنده، نیابت اتباع دولت فرستنده یا اتخاذ تدابیری به‌منظور تضمین نیابت مناسب آنان نزد محاکم و یا مقام‌های دولت پذیرنده جهت تصویب تدابیر موقتی به قصد حفظ حقوق و منافع این افراد، زمانی که آنان به علت عدم حضور نمی‌توانند در زمان مناسب از حقوق و منافع خود دفاع نمایند؛

د- ابلاغ اسناد قضایی و فراقضایی یا اجرای نیابت‌های قضایی طبق موافقت‌نامه‌های بین‌المللی لازم‌الاجرا یا در صورت عدم وجود چنین موافقت‌نامه‌هایی، به هر شکلی که منطبق با قوانین و مقررات دولت پذیرنده باشد؛

ذ- اجرای حق نظارت و بازرسی پیش‌بینی شده در قوانین و مقررات دولت‌فرستنده بر کشتی‌های دریایی و قایق‌های رودخانه‌ای دارنده تابعیت دولت فرستنده و بر هواپیماهای ثبت شده در آن دولت و همچنین بر خدمه آن‌ها؛

ر- کمک به کشتی‌ها، قایق‌ها و هواپیماهای پیش‌گفته و خدمه آن‌ها، در بند «ک» این ماده دریافت اظهارنامه‌های مربوط به سفر این کشتی‌ها و قایق‌ها و بررسی و ملاحظه اسناد موجود در آن‌ها، با رعایت صلاحیت مقام‌های دولت پذیره انجام تحقیقات در مورد حوادثی که در طول سفر رخ داده‌اند و حل و فصل هرگونه اعتراض مطروح فی‌مابین کاپیتان و افسران و ناوی‌ها در صورتی که قوانین و مقررات دولت فرستنده چنین اجازه‌ای را پیش‌بینی کرده باشد و

ز- اجرای کلیه اشتغالات دیگری که از سوی دولت فرستنده به پست کنسولی واگذار شده‌اند، در صورتی که قوانین و مقررات دولت پذیرنده آن‌ها را ممنوع نکرده باشند و یا این دولت با آن‌ها مخالفت ننماید و یا در موافقت‌نامه‌های بین‌المللی لازم‌الاجرا فی‌مابین دولت‌های فرستنده و پذیرنده پیش‌بینی شده باشند.

1. United Kingdom, Official Secrets Act 1911, s 1. Retrieved January 3, 2025 from https:// www. legislation. gov.uk/ukpga/1911/28/pdfs/ukpga_19110028_en.pdf; United States, United States Code: Espionage and Censorship, 18 USC §792–799, (1982). Retrieved January 3, 2025 from https://www.loc.gov/item/uscode1982-047018037.

یا کنسولی ناسازگار هستند، مورد استفاده قرار گیرند؛ ب- نمایندگان دیپلماتیک و مأموران کنسولی نباید در فعالیت‌های سایبری شرکت کنند که در امور داخلی دولت پذیرنده مداخله کرده یا با قوانین و مقررات آن دولت ناسازگار باشد». برای نمونه، دولت فرستنده نمی‌تواند از اماکن هیأت دیپلماتیک خود برای انجام جاسوسی سایبری علیه دولت پذیرنده استفاده کند.[۱] همچنین استفاده از زیرساخت سایبری یک هیأت دیپلماتیک برای انجام فعالیت‌های تجاری مانند تجارت الکترونیکی نیز نمی‌تواند به‌عنوان یک وظیفه دیپلماتیک محسوب شود.

مسئله جداگانه‌ای مطرح است که آیا دولت فرستنده می‌تواند بدون رضایت دولت پذیرنده، از اماکن هیأت دیپلماتیک یا پست کنسولی خود به‌عنوان پایگاهی برای انجام جاسوسی سایبری علیه دولت ثالث استفاده کند یا نه؟ چه این جاسوسی علیه نهادهای دولت ثالث در دولت پذیرنده انجام شود یا خارج از آن. اکثریت کارشناسان راهنمای تالین ۲ بر این باور بودند که چنین اقداماتی طبق بند (الف) این قاعده ممنوع است، زیرا با وظایف پذیرفته‌شده دیپلماتیک ناسازگار است. عده‌ای از کارشناسان این نظر را رد و استدلال کردند که روابط دیپلماتیک ماهیتی دوجانبه دارند و تعهداتی در قبال دولت‌های ثالث ایجاد نمی‌کنند. افزون بر این، آن‌ها اشاره کردند که رویه دولت‌ها و ابراز باور حقوقی کافی برای نتیجه‌گیری، دائر بر این‌که چنین ممنوعیتی به حقوق بین‌الملل عرفی تبدیل شده است، وجود ندارد. به‌طور خاص آن‌ها به اتهامات طولانی‌مدت دائر بر رویه دولت‌ها که برخلاف این ممنوعیت است، اشاره کردند.[۲] با این حال، نگارندگان هم‌سو با اکثریت

---

۱. به بحث‌های مربوط به قاعده ۴۱ راهنمای تالین ۲ مراجعه کنید. همچنین در این راستا دولت اتریش بیان داشته است: «آرشیوها، اسناد و مکاتبات رسمی یک نمایندگی دیپلماتیک یا کنسولی یا دفتر اطلاعاتی که به‌صورت الکترونیکی باشد از تعرض مصون است. نمایندگی‌های دیپلماتیک و کنسولی و همچنین سازمان‌های بین‌المللی (با رعایت مفاد توافق‌نامه مقر خود) نباید در فعالیت‌های سایبری برخلاف قوانین و مقررات دولت پذیرنده، از جمله فعالیت‌های جاسوسی شرکت کنند و نباید در امور داخلی آن کشور مداخله کنند. علاوه بر این، اماکن آن‌ها نباید برای شرکت در فعالیت‌های سایبری که با عملکرد آن‌ها ناسازگار است، استفاده شود».

Position Paper of the Republic of Austria: Cyber Activities and International Law, op.cit., p. 14..

2. Ibid.

کارشناسان هستند؛ چراکه اگر این فعالیت‌ها را ناقض و برخلاف ذات فعالیت‌های آنان ندانیم، باعث می‌شود که رویه‌ای در استفاده غیرقانونی و مخرب علیه حاکمیت سایر دولت‌ها در زیر چتر مصونیت آنان به‌وجود آید.

از سوی دیگر، آن‌چه در بند (ب) این قاعده منعکس شده، این واقعیت است که وظیفه مأموران دیپلماتیک و کنسولی احترام به قوانین و مقررات دولت پذیرنده است.[۱] به‌عنوان مثال در بیشتر موارد، اقدام یک مأمور دیپلماتیک به سرقت آنلاین مالکیت فکری در قلمرو دولت پذیرنده نقض بند (ب) خواهد بود، زیرا چنین فعالیت‌هایی به احتمال زیاد قوانین و مقررات دولت پذیرنده را نقض می‌کند.[۲] همچنین مطابق با بند (ب)، مأموران دیپلماتیک و کنسولی از دخالت در امور داخلی دولت پذیرنده منع شده‌اند.[۳] برای مثال مأموران دیپلماتیک نمی‌توانند از شبکه‌های اجتماعی برای برنامه‌ریزی برکناری دولت پذیرنده یا مشارکت در «کارزارهای سیاسی» استفاده کنند. از سوی دیگر، آن‌ها می‌توانند برای «حمایت از منافع کشور متبوع خود یا اتباع آن مطابق با حقوق بین‌الملل» در فعالیت‌های سایبری شرکت کنند.[۴] به‌عنوان نمونه، کارشناسان توافق داشتند که مأموران دیپلماتیک می‌توانند از شبکه‌های اجتماعی برای درخواست آزادی اتباع خود از بازداشت دولت – پذیرنده استفاده کنند، به شرطی که بازداشت را غیرقانونی یا به‌نحوی نامناسب بدانند؛ آن‌ها این دیدگاه را که چنین اقدامی دخالت در امور داخلی است، رد کردند.[۵]

با توجه به مصونیت مأموران دیپلماتیک از فرآیندهای کیفری، مدنی و اداری دولت پذیرنده[۶]، نمی‌توان این مأموران را به‌دلیل انجام فعالیت‌هایی که ناقض این قاعده باشد، تحت صلاحیت قضایی یا اجرایی قرار داد.[۷] با این حال آن‌ها می‌توانند به‌عنوان شخص

---

۱. ماده ۴۱ (۱) کنوانسیون روابط دیپلماتیک؛ ماده ۵۵ (۱) کنوانسیون روابط کنسولی.

2. Tallinn Manual 2.0, op.cit, at 229.

۳. ماده ۴۱ (۱) کنوانسیون روابط دیپلماتیک؛ ماده ۵۵ (۱) کنوانسیون روابط کنسولی.

4. Yearbook of the International Law Commission, op.cit., p. 104.

5. Tallinn Manual 2.0, op.cit., at 229-230.

۶. مطابق با قاعده ۴۴ راهنمای تالین ۲.

۷. مطابق با قواعد ۸–۹ راهنمای تالین ۲.

نامطلوب[۱] اعلام شوند که در این‌صورت دولت فرستنده موظف خواهد بود آن‌ها را فرا بخواند.[۲]

در نهایت، هر دو کنوانسیون وین درباره روابط دیپلماتیک و روابط کنسولی، تصریح می‌کنند که یک هیأت دیپلماتیک یا پست کنسولی تنها با رضایت دولت پذیرنده می‌تواند «فرستنده بی‌سیم»[۳] نصب و استفاده کند.[۴] در زمان تدوین این کنوانسیون‌ها، فرستنده‌های بی‌سیم عمدتاً برای ارسال امواج رادیویی به‌کار می‌رفتند. کارشناسان راهنمای تالین ۲ نظر دادند که این زبان معاهده تا حدی قدیمی است و ترجمه دقیق آن به فناوری‌های سایبری کاملاً روشن نیست. به‌ویژه کارشناسان بر این نظر بودند که تجهیزاتی که به‌طور کلی سیگنال‌های رادیویی را فقط در محدوده محیط یک هیأت دیپلماتیک یا پست کنسولی منتشر می‌کنند مانند روترهای بی‌سیم[۵]، مشمول این قاعده نمی‌شوند. اما کارشناسان توافق داشتند که با ظهور انواع جدید فناوری‌های بی‌سیم، این اصل باید همچنان نیازمند رضایت دولت‌پذیرنده برای نصب و استفاده از تجهیزاتی باشد که امکان ارسال ارتباطات فراتر از محدوده هیأت دیپلماتیک یا پست کنسولی را فراهم می‌کند. این امر شامل نصب انواع تجهیزات ارتباطی بی‌سیم (مانند تجهیزات ارتباطات ماهواره‌ای[۶]) می‌شود، مشروط بر این که استفاده از آن‌ها قابلیت ایجاد تداخل مضر[۷] با ارتباطات بی‌سیم در دولت پذیرنده را داشته باشد.[۸]

---

1. Persona Non Grata.

اعلان شخص نامطلوب آن دیپلمات‌هایی که بدون مدرک قوی مظنون به فعالیت‌های دیگر علیه منافع دولت پذیرنده هستند نیز قانونی است، زیرا تصمیم دولت پذیرنده کاملاً اختیاری است و نیازی به ارائه هیچ دلیلی ندارد. برای مطالعه بیشتر به منبع زیر مراجعه نمایید؛

Jean D'Aspremont, *Persona Non Grata* (in Wolfrum, R. (ed), Max Planck Encyclopedia of Public International Law, 2009).

2. Tallinn Manual 2.0, op.cit., at 230.

3. Wireless Transmitter

۴. ماده ۲۷ (۱) کنوانسیون روابط دیپلماتیک؛ ماده ۳۵ (۱) کنوانسیون روابط کنسولی.

5. Wireless Router.

6. Satellite Communications.

۷. در خصوص تداخل مضر، به قاعده ۶۳ راهنمای تالین ۲ نیز مراجعه شود.

8. Tallinn Manual 2.0, op.cit., at 230.

۶-۲. مزایا و مصونیت‌های مأموران دیپلماتیک و کنسولی[۱]

مصونیت دیپلماتیک، در واقع اولین اصلی است که در حقوق بین‌الملل دیپلماتیک حول محور آن شکل گرفته است. این مصونیت‌ها اغلب ماهیت عرفی دارند و ماده ۲۹ کنوانسیون روابط دیپلماتیک[۲] آن‌ها را مورد تأیید و تصدیق مجدد قرار داده است.[۳] با این حال، ماموران دیپلماتیک مکلف به احترام و رعایت قوانین و مقررات دولت پذیرنده هستند، به استثنای مواردی که مزایا و یا مصونیت‌ها، آنان را از چنین تکلیفی معاف می‌نماید؛[۴] چراکه در صورت سوءاستفاده از این حق، با ضمانت اجراهای حقوق بین‌الملل روبرو خواهند شد. برای نمونه، دولت پذیرنده می‌تواند هر آن و بی‌آن‌که الزامی به توجیه تصمیم خود داشته باشد به کشور فرستنده اطلاع دهد که رئیس یا هر یک از اعضای دیپلماتیک مأموریت (شخص نامطلوب)[۵] است و یا آنکه هر یک از سایر اعضای کارکنان مأموریت،

---

۱. بسیاری از مصونیت‌های ذکر شده در این بخش، به میزان محدودتری شامل اعضای خانواده کارکنان مأموریت دیپلماتیک یا پست کنسولی، همچنین کارکنان اداری و فنی مأموریت یا پست و خانواده‌های آنان می‌شود (برای نمونه مواد ۳۷-۳۸ کنوانسیون روابط دیپلماتیک و ماده ۴۳ کنوانسیون روابط کنسولی). با این حال، توضیحاتی که در ادامه ارائه شده است، این مصونیت‌ها را بررسی نمی‌کند (کنوانسیون وین درباره روابط دیپلماتیک، کنوانسیون وین درباره روابط کنسولی و کنوانسیون مأموریت‌های ویژه، دامنه خاص این مصونیت‌ها را که به این افراد اعطا شده است، تعیین کرده‌اند و برای آگاهی بیشتر باید به این اسناد مراجعه شود. همچنین در مورد مصونیت دولت‌ها و مقامات دولتی تحت حقوق بین‌الملل عمومی، به قاعده ۱۲ راهنمای تالین ۲ مراجعه کنید).

۲. ماده بیست و نهم: «مأمور دیپلماتیک مصون از تعرض است و نمی‌توان او را به هیچ عنوان مورد توقیف یا بازداشت قرارداد. کشور پذیرنده با وی رفتار محترمانه‌ای که در شان او است خواهد داشت و اقدامات لازم را برای ممانعت از وارد آمدن لطمه به شخص و آزادی و حیثیت او اتخاذ خواهد کرد».

۳. بیگ‌زاده، پیشین، صص ۸۹۱-۸۹۲.

۴. همان، ص ۸۷۴.

۵. اعلام به‌عنوان شخص نامطلوب یک راه‌حل خاص تحت کنوانسیون روابط دیپلماتیک است.

United States of America v. Iran, op.cit., para 85.

با این حال، این روش تنها راه‌حل موجود نیست. برای نمونه در صورتی که عملیات دولت فرستنده منجر به یک عمل متخلفانه بین‌المللی شود، دولت پذیرنده احتمالاً می‌تواند در پاسخ خود از اقدامات متقابل استفاده کند.

D'Aspremont, op.cit., para 16.

برای مطالعه بیشتر رجوع نمایید به سید مصطفی میرمحمدی، «سوءاستفاده از مصونیت‌های دیپلماتیک و ضمانت اجرای آن در حقوق بین‌الملل»، دوفصلنامه علمی حقوق تطبیقی، شماره ۳، (۱۳۸۱)، صص ۱۴۴ به بعد.

مورد قبول نیست؛ در این صورت دولت فرستنده آن شخص را بر حسب مورد فرا خواهد خواند و یا به خدمت وی در مأموریت پایان خواهد داد.[۱]

قاعده ۴۴ راهنمای تالین ۲ بیان می‌دارد: «تا جایی‌که مأموران دیپلماتیک و مأموران کنسولی از مصونیت‌های کیفری، مدنی و اداری برخوردارند، این مصونیت‌ها شامل فعالیت‌های سایبری آن‌ها نیز می‌شود». لذا این قاعده مصونیت‌هایی را که مأموران دیپلماتیک و کنسولی از آن بهره‌مند هستند، بیان می‌کند. البته این مصونیت‌ها همواره قابل چشم‌پوشی توسط دولت فرستنده می‌باشند.[۲]

بنابراین مادامی‌که مأموران دیپلماتیک در آن کشور حضور دارند در برابر صلاحیت کیفری دولت پذیرنده برای هر فعالیتی که تحت قوانین داخلی دولت پذیرنده به‌عنوان جرم سایبری تلقی شود، از مصونیت برخوردارند.[۳] این مصونیت دیپلماتیک مطلق و بی‌قیدوشرط است. آن‌ها همچنین از مصونیت در برابر بازداشت برخوردارند و از تعهد به ادای شهادت به‌عنوان شاهد معاف هستند.[۴] پس از اتمام وظایف دیپلماتیک و خروج از دولت پذیرنده، این مزایا و مصونیت‌ها معمولاً پایان می‌یابد، هرچند مصونیت برای اعمال انجام‌شده در اجرای وظایف رسمی همچنان باقی می‌ماند.[۵] همچنین مأموران دیپلماتیک از مصونیت در برابر صلاحیت‌های مدنی و اداری دولت پذیرنده در رابطه با فعالیت‌های سایبری خود برخوردارند، مگر در موارد خاصی که مربوط به اموال غیرمنقول خصوصی، ارث یا هرگونه فعالیت حرفه‌ای یا تجاری مامور دیپلماتیک باشد که در زمان حضور در دولت پذیرنده و خارج از وظایف رسمی وی انجام شده باشد.[۶] به‌عنوان مثال مأمور

---

۱. ماده ۹ کنوانسیون روابط دیپلماتیک.

۲. ماده ۳۲ (۱) کنوانسیون روابط دیپلماتیک؛ ماده ۴۵ (۱) کنوانسیون روابط کنسولی.

۳. ماده ۳۱ (۱) کنوانسیون روابط دیپلماتیک؛ همچنین مطابق ماده ۳۷ کنوانسیون روابط دیپلماتیک، بستگان نماینده دیپلماتیک، کارمندان اداری و فنی و سایر افراد مرتبط با این ماموریت از امتیازات و مصونیت‌های خاصی برخوردار هستند.

۴. ماده ۲۹ و ۳۱ (۲) کنوانسیون روابط دیپلماتیک.

۵. ماده ۳۹ (۲) کنوانسیون روابط دیپلماتیک؛ قاعده ۱۲ راهنمای تالین ۲.

۶. ماده ۳۱ (۱) کنوانسیون روابط دیپلماتیک.

دیپلماتیک ممکن است در صورت فروش کالا به‌صورت آنلاین به‌عنوان یک فعالیت تجاری شخصی، از مصونیت در برابر صلاحیت مدنی یا اداری برخوردار نباشد.

از سوی دیگر مبنای مصونیت و مزایای کنسولی همانند مصونیت‌ها و مزایای دیپلماتیک بر نظریه «حسن خدمت» مبتنی است. ماده ۲۸ کنوانسیون روابط کنسولی اعلام می‌دارد که دولت پذیرنده کلیه تسهیلات لازم را برای انجام اشتغالات در اختیار پست کنسولی قرار می‌دهد. بنابراین در یک نگاه کلی مشاهده می‌شود که گستره مصونیت‌های کنسولی محدودتر از مصونیت‌های دیپلماتیک است.[۱] از این‌رو مأموران کنسولی از مصونیت محدودتری در برابر صلاحیت کیفری و مدنی دولت پذیرنده در رابطه با فعالیت‌های سایبری خود برخوردارند.[۲] به‌ویژه آن‌ها از مصونیت مطلق در برابر صلاحیت کیفری دولت پذیرنده برخوردار نیستند؛ اما نمی‌توان آن‌ها را بازداشت یا زندانی کرد مگر در مورد ارتکاب یک جرم سنگین و آن‌هم بر اساس تصمیم یک مرجع قضایی صلاحیت‌دار.[۳]

نتیجه‌گیری

فضای سایبر به‌طور مداوم در حال پیشرفت است و با توجه به پتانسیل بالای آن برای رشد، هرگونه اتفاقی قابل رخ داد در آینده خواهد بود. دیپلماسی سایبری اکنون به بخش جدایی‌ناپذیر از زندگی روزمره دیپلمات‌ها و کنسول‌ها تبدیل شده است. در این محیط جدید، حقوق سنتی دیپلماسی نیز باید از طریق تفسیرهای جدید از قواعد موجود تکامل یابد و اگر برخی از این قواعد برای تنظیم دیپلماسی اینترنتی ناکافی یا ناقص باشند، باید قواعد جدیدی ایجاد شوند. با این حال همان‌طور که در مقاله به تفصیل مورد مداقه قرار گرفت؛ نخست، مأموریت‌های دیپلماتیک و کنسولی از غیرقابل تعرض بودن اماکن خود طبق حقوق بین‌الملل عرفی، همان‌طور که در کنوانسیون وین درباره روابط دیپلماتیک و

---

۱. بیگ‌زاده، پیشین، صص ۹۱۶-۹۱۷.

۲. در مقایسه ماده ۲۹ کنوانسیون روابط دیپلماتیک با مواد ۴۱، ۴۳ و ۴۴ کنوانسیون روابط کنسولی.

۳. ماده ۴۱ کنوانسیون روابط کنسولی؛ البته توجه داشته باشید که مأموران کنسولی از مصونیت رسیدگی کیفری برخوردار نیستند (ماده ۶۳ کنوانسیون روابط کنسولی).

کنوانسیون وین درباره روابط کنسولی تدوین شده است، برخوردارند. اماکن یک مأموریت غیرقابل تعرض هستند و مأموران دولت میزبان نباید بدون رضایت رئیس مأموریت وارد این اماکن شوند. علاوه بر این هرگونه اموالی که در داخل مأموریت قرار دارد –از جمله زیرساخت‌های فناوری اطلاعات و ارتباطات (ICT) –از تفتیش، مصادره، توقیف یا اجرای احکام قضایی مصون هستند. این بدان معناست که دسترسی از راه دور به زیرساخت‌های فناوری اطلاعات و ارتباطات مستقر در داخل ماموریت بدون رضایت صریح نیز ممنوع است. علاوه بر این، آرشیوها و اسناد همچنین مکاتبات رسمی مأموریت، حتی به‌صورت الکترونیکی در هرکجا که باشند غیرقابل تعرض هستند. علاوه برآن، دولت پذیرنده وظیفه دارد آزادی ارتباطات ماموریت را برای تمامی اهداف ممکن سازد.

در پایان، همه افرادی که از امتیازات و مصونیت‌ها بهره‌مند هستند، وظیفه دارند قوانین و مقررات دولت پذیرنده را رعایت کنند و در امور داخلی آن دولت دخالت نکنند. علاوه بر این، اماکن مأموریت نباید به‌نحوی استفاده شوند که با وظایف مأموریت یا سایر قواعد حقوق بین‌الملل عام یا هر توافق خاصی که بین دولت فرستنده و دولت پذیرنده برقرار است، ناسازگار باشد. در زمینه سایبری، این امر همچنین بدان معناست افرادی که از امتیازات و مصونیت‌ها بهره‌مند هستند، نباید در فعالیت‌های نظارت غیرقانونی یا جاسوسی در دولت پذیرنده شرکت کنند و اماکن ماموریت نیز نباید برای چنین مقاصدی استفاده شوند. در این راستا دولت پذیرنده وظیفه دارد تمامی اقدامات مناسب را برای حفاظت از ماموریت در برابر هرگونه نفوذ یا آسیب و جلوگیری از هرگونه اختلال در آرامش مأموریت یا خدشه به حیثیت آن انجام دهد. بنابراین دولتی که از یک فعالیت مخرب سایبری علیه یک ماموریت دیپلماتیک یا کنسولی در قلمرو خود آگاه شود، باید تمامی اقدامات مناسب را برای حفاظت از ماموریت در برابر چنین فعالیتی انجام دهد.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID
Kian Biglarbeigi https://orcid.org/0000-0001-8659-0299
Sattar Azizi https://orcid.org/0000-0003-3609-7644

منابع

کتاب‌ها

- بیگ‌زاده، ابراهیم، *حقوق بین‌الملل*، جلد دوم: روابط تابعان، چاپ اول (تهران: بنیاد حقوقی میزان، ۱۴۰۱).
- صدر، جواد، *حقوق دیپلماتیک و کنسولی*، چاپ شانزدهم (تهران: مؤسسه انتشارات دانشگاه تهران، ۱۳۹۸).

مقاله‌ها

- توسلی نایینی، منوچهر و قریشی، امیرهمایون، «وضعیت حقوقی پیک و کیسه دیپلماتیک در حقوق بین‌الملل»، فصلنامه سیاست خارجی، سال ۲۴، شماره ۳، (۱۳۸۹).
- توسلی‌نایینی، منوچهر، «آزادی ارتباطات مأموریت‌های دیپلماتیک در حقوق بین‌الملل و جایگاه حقوقی پیک و کیسه دیپلماتیک در آن»، فصلنامه تحقیقات حقوقی، دوره ۱۹، شماره ۷۳، (۱۳۹۵).
- میرمحمدی، سیدمصطفی، «سوءاستفاده از مصونیت‌های دیپلماتیک و ضمانت اجرای آن در حقوق بین‌الملل»، دوفصلنامه علمی حقوق تطبیقی، دوره ۰، شماره ۳، (۱۳۸۱).

پایان‌نامه

- بیگلربیگی، کیان، حملات سایبری و نقض اصل عدم مداخله، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، به راهنمایی ابراهیم بیگ‌زاده، دانشگاه شهید بهشتی، (۱۴۰۲).

References

Books

- Choi, Won-Mog, *Diplomatic and Consular Law in the Internet Age* (Singapore: Year Book of International Law, 2006).

- D'Aspremont, Jean, *Persona Non Grata* (in Wolfrum, R. (ed), Max Planck Encyclopedia of Public International Law, 2009).

- Denza, Eileen, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*, 4th Edition (Oxford: Commentaries on International Law, 2016).

- Garner, Bryan A, *Black's Law Dictionary*, 8th Edition (USA: Thomson West, 1990).

- International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation* (Cambridge University Press, 2017).

- International Law Commission, *Yearbook of the International Law Commission*, Vol. II (United Nations, 1958).

- Kershaw, Anthony, *First Report from the Foreign Affairs Committee, Session 1984–85: the Abuse of Diplomatic Immunities and Privileges* (in Great Britain, Parliament, House of Commons, Foreign Affairs Committee, H.M. Stationery Office, 1984).

- Libicki, Martin C, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).

- Liivoja, Rain & McCormack, Tim, *Law in Virtual Battlespace: The Tallinn Manual and the jus in bello* Vol. 15 (Yearbook of International Humanitarian Law, 2013).

- Roscini, Marco, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014).

- Wouters, Jan, Duquet, Sanderijn & Meuwissen, Katrien, *The Vienna Conventions on Diplomatic and Consular Relations*, in Cooper, Andrew F., Heine, Jorge & Thakur, Ramesh (eds) (The Oxford Handbook of Modern Diplomacy, 2013).

Articles

- Minnaar, Anthony, "Protection of Foreign Missions in South Africa", African Security Review, Vol. 9, No. 2, (2000).

- Wallace, David A & Visger, Mark, "Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community", Journal of Law & Cyber Warfare, Vol. 6, No. 2, (2018).

Conventions and Documents

- Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System, (2003), Retrieved November 17, 2024 from https://rm.coe.int/168008160f .

- Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, (1947), Retrieved January 1, 2025 from https:// digitallibrary. un.org/ record/ 210063? v=pdf.

- Australian Government, Department of Foreign Affairs and Trade, Protocol Guidelines. Retrieved January 4, 2025 from https:// www. dfat. gov.au/about-us/ publications/ corporate/ protocol- guidelines.

- Convention on Cybercrime (Budapest Convention), Council of Europe, European Treaty Series – No. 185., (2001), Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https:// rm.coe. int/ 1680081561.

- Convention on Jurisdictional Immunities of States and Their Property, (2004). Retrieved January 4, 2025 from https:// treaties. un. org/ doc/ source/recenttexts/english_3_13.pdf.

- Convention on Special Missions, (1969). Retrieved January 3, 2025 from https:// legal. un. org/ ilc/ texts/ instruments/ english/ conventions/ 9_3_1969.pdf.

- Convention on the Privileges and Immunities of the United Nations, (1946). Retrieved January 1, 2025 from https:// treaties. un. org/ pages/ View Details. aspx? src= TREATY& mtdsg_ no= III-1&chapter= 3&clang=_en.

- Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, (2001). Retrieved January 3, 2025 from https:// legal. un. org/ ilc/ texts/ instruments/ english/ commentaries/ 9_6_2001.pdf.

- Draft Articles on the Status of the Diplomatic Courier and the Diplomatic Bag Not Accompanied by Diplomatic Courier and Draft Optional Protocols, (1989). Retrieved January 3, 2025 from https:// legal. un. org/ilc/texts/instruments/english/draft_articles/9_5_1989.pdf.

- Headquarters Agreement between the International Criminal Court and the Host State, (2007), Retrieved January 2, 2025 from https://www.icc-cpi.int/news/headquarters-agreement-between-international-criminal-court-and-host-state.

- Position Paper of the Republic of Austria: Cyber Activities and International Law, (2024). Retrieved January 3, 2025 from https://

docs- library. unoda. org/ Open-Ended_ Working_ Group_ on_ Information_and_Communication_Technologies_-_(2021)/ Austrian_ Position_Paper_-_Cyber_ Activities_ and_ International_ Law_ (Final_ 23.04. 2024).pdf.

- Rome Statute of the International Criminal Court, (1998). Retrieved January 1, 2025 from https:// www. ohchr. org/ en/ instruments-mechanisms/instruments/rome-statute-international-criminal-court.

- United Kingdom, Official Secrets Act 1911. Retrieved January 3, 2025 from https:// www. legislation. gov.uk/ ukpga/1911/28/ pdfs/ukpga_ 19110028_en.pdf.

- United Nations Charter, (1945), Retrieved September 12, 2024 from https://www.un.org/en/about-us/un-charter/full-text.

- United Nations Conference on Diplomatic Intercourse and Immunities, United States of America: amendment to article 22 (A/CONF. 20/C.1/L.153), (1961). Retrieved January 4, 2025 from https:// legal. un.org/ diplomaticconferences/ 1961_dipl_ intercourse/ docs/ english/ vol_2.pdf.

- United Nations Conference on Diplomatic Intercourse and Immunities, Official Records (A/CONF.20/14), (1961), Retrieved January 4, 2025 from https:// documents. un. org/ doc/ undoc/ gen/ g62/016/03/ pdf/ g6201603.pdf.

- United States, United States Code: Espionage and Censorship, 18 USC §792–799, (1982), Retrieved January 3, 2025 from https:// www. loc.gov/item/uscode1982-047018037.

- US Department of State Office of the Legal Advisor, Digest of United States Practice in International Law, (2000), Retrieved January 4, 2025 from https://2009-2017.state.gov/s/l/c8185.htm.

- Vienna Convention on Consular Relations, (1963), Retrieved January 3, 2025 from https:// legal.un. org/ilc/ texts/ instruments/ english/ conventions/ 9_2_1963.pdf.

- Vienna Convention on Diplomatic Relations, (1961), Retrieved January 3, 2025 from https:// legal.un.org/ ilc/texts/ instruments/ english/ conventions/ 9_1_1961.pdf.

Cases

- Alcom v. Republic of Colombia, House of Lords, 1984. Retrieved January 4, 2025 from https://vlex.co.uk/vid/alcom-ltd-v-republic-792878269.

- Equatorial Guinea v. France, Immunities and Criminal Proceedings Case, ICJ, Merits, Judgment, 2020. Retrieved January 3, 2025 from https://www.icj-cij.org/case/163.

- Finzer v. Barry: United States Court of Appeals for the District of Columbia Circuit, Court of Appeals of the United States, 1986. Retrieved January 4, 2025 from https://casetext.com/case/finzer-v-barry.

- Ignatiev v. United States: United States Court of Appeals for the District of Columbia Circuit, Court of Appeals of the United States. 2001. Retrieved January 4, 2025 from https://casetext.com/case/ignatiev-v-us.

- Liberian Eastern Timber Corp. v. The Government of Liberia, ICSID, 1987. Retrieved January 4, 2025 from https:// www. italaw. com/ cases/3545.

- Minister for Foreign Affairs and Trade and others v. Magno and another, Federal Court of Australia, 1992. Retrieved January 4, 2025 from https://ihl-databases.icrc.org/en/national-practice/geraldo-magno-ines-almeida-v-minister-foreign-affairs-and-trade-commissioner.

- MK v. State Secretary for Justice, Council of State, President of the Judicial Division, 1988. Retrieved January 4, 2025 from http:// www. cahdidatabases.coe.int/Contribution/Details/192.

- Nicaragua v. United States of America, Military and Paramilitary Activities in and against Nicaragua, ICJ, Judgment, 1986, para 186. Retrieved January 9, 2025 from https://www.icj-cij.org/case/70.

- R (Bancoult) v. Secretary of State for Foreign and Commonwealth Affairs, Court of Appeal of United Kingdom, Judgment, 2014. Retrieved January 4, 2025 from https://vlex.co.uk/vid/r-on-the-application-793368225.

- Republic of 'A' Embassy Bank Account Case, Supreme Court (Austria), (1986), Retrieved January 4, 2025 from https://www.cambridge.org/ core/journals/ international- law-reports/ article/ abs/ republic- of-a- embassy- bank-account- case/ D34423E41E557EAE87C9E2E98E7CE707.

- United States of America v. Iran, United States Diplomatic and Consular Staff in Tehran, ICJ, Judgments, 1980.Retrieved January 3, 2025 from https://www.icj-cij.org/case/64.

In Persian

Books

- Beigzadeh, Ebrahim, *International Law*, Volume Two: Relations between Subjects, First Edition (Tehran: Mizan Legal Foundation, 1401). [In Persian]

- Sadr, Javad, *Diplomatic and Consular Law*, 16th Edition (Tehran: Tehran University Publishing House, 2019). [In Persian]

Articles

- Mirmohammadi, Seyed Mostafa, "Abuse of Diplomatic Immunities and Guarantee of Its Enforcement in International Law", Comparative Law Bi-Quarterly, Vol. 0, No. 3, (2002). [In Persian]

- Tavasli-Naini, Manouchehr & Qureshi, Amir Homayoun, "The Legal Status of Diplomatic Couriers and Bags in International Law," Foreign Policy Quarterly, Vol. 24, No. 3, (2010). [In Persian]

- Tavasoli Naini, Manouchehr, "Freedom of Communication of Diplomatic Missions in International Law and the Legal Status of Diplomatic Couriers and Bags in It", Shahid Beheshti University Legal Research Quarterly, Vol. 19, No. 73, (2016). [In Persian]

Thesis

- Biglarbeigi, Kian, Cyberattacks and Violation of the Principle of Non-Intervention, Master's Thesis in International Law, Supervised by Ebrahim Beigzadeh Tehran, Shahid Beheshti University, Faculty of Law, (1402). [In Persian]

استناد به این مقاله: بیگلربیگی، کیان و عزیزی، ستار، «مواجهه حقوق دیپلماتیک و کنسولی با عملیات سایبری رد پرتو راهنمای تالین ۲»، پژوهش حقوق عمومی، دوره ۲۸، شماره ۹۱، (۱۴۰۵)، ۲۲۷-۲۸۴.

Doi: 10.22054/qjpl.2025.83725.3067