Cyber Warfare and Diplomatic Immunity: Evaluating State and Non-State Cyber Operations Targeting Diplomats Under Indonesian Law

Author:

Arya Putra Mahendra[1], Heribertus Jaka Triyana[2]

ABSTRACT

In the 21st century, cyber warfare has emerged as a critical threat to international diplomacy, with state and non-state actors increasingly targeting embassies and diplomats through espionage, data theft, and network intrusions. Traditional diplomatic protections under the Vienna Convention on Diplomatic Relations (1961) including the inviolability of mission premises, archives, and communications were formulated in a pre digital era and do not explicitly address cyber operations. This research examines how these principles can be interpreted and applied to cyberspace, and to what extent Indonesian law provides legal protection for foreign diplomatic missions against such threats.

Using a normative juridical (doctrinal) approach complemented by comparative and analytical methods, this study draws upon primary legal materials such as the ITE Law (Law No. 11 of 2008, as amended), Personal Data Protection Law (Law No. 27 of 2022), Foreign Relations Law (Law No. 37 of 1999), and Presidential Regulation No. 82 of 2022 alongside international instruments and cybersecurity case studies. The analysis reveals that Indonesia's legal framework criminalizes unauthorized access and interception but does not explicitly classify embassies as specially protected entities in cyberspace. Furthermore, fragmented institutional coordination among BSSN, the Ministry of Foreign Affairs, Polri, and TNI limits the effectiveness of enforcement.

At the international level, the study finds that the Vienna Convention's inviolability principles can logically extend to digital archives and communications; however, enforcement is hindered by attribution difficulties, the espionage grey zone, and political reluctance to confront powerful actors. The research concludes that Indonesia's current framework offers partial but incomplete protection. It recommends revising national laws to explicitly include diplomatic missions within the scope of cyber protection, establishing embassy specific Standard Operating Procedures (SOPs), and enhancing cooperation at the ASEAN and UN levels to strengthen the protection of diplomatic entities in cyberspace.

Keywords: Cyber Warfare, Diplomatic Immunity, Vienna Convention, Indonesian Law, Cyber Espionage, BSSN, Inviolability Principles

---

[1] Student at the Department of International Law, Faculty of Law, Universitas Gadjah Mada (International Undergraduate Program 2021).
[2] Lecturer at the Department of International Law, Faculty of Law, Universitas Gadjah Mada.

Perang Siber dan Kekebalan Diplomatik: Evaluasi Operasi Siber oleh Aktor Negara dan Non-Negara yang Menargetkan Diplomat Berdasarkan Hukum Indonesia

Penulis:

Arya Putra Mahendra[3], Heribertus Jaka Triyana[4]

INTISARI

Pada abad ke-21, perang siber telah muncul sebagai ancaman serius terhadap diplomasi internasional, dengan aktor negara maupun non-negara semakin sering menargetkan kedutaan dan diplomat melalui kegiatan spionase, pencurian data, serta peretasan jaringan. Perlindungan diplomatik tradisional yang diatur dalam Konvensi Wina tentang Hubungan Diplomatik (1961) terutama asas inviolability terhadap gedung misi, arsip, dan komunikasi diplomatik disusun sebelum era digital dan belum secara eksplisit mengatur operasi siber. Penelitian ini mengkaji bagaimana prinsip-prinsip tersebut dapat diinterpretasikan dan diterapkan dalam konteks siber, serta sejauh mana hukum nasional Indonesia memberikan perlindungan hukum terhadap misi diplomatik asing dari ancaman tersebut.

Dengan menggunakan pendekatan yuridis normatif (doktrinal) yang dilengkapi dengan metode komparatif dan analitis, penelitian ini menggunakan bahan hukum primer seperti Undang-Undang ITE (UU No. 11 Tahun 2008 jo. UU No. 1 Tahun 2024), Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), Undang-Undang Hubungan Luar Negeri (UU No. 37 Tahun 1999), serta Peraturan Presiden No. 82 Tahun 2022, bersama dengan instrumen internasional dan studi kasus serangan siber terhadap entitas diplomatik. Hasil analisis menunjukkan bahwa kerangka hukum Indonesia telah mengkriminalisasi akses tidak sah dan penyadapan elektronik, namun belum secara tegas mengakui kedutaan sebagai entitas yang dilindungi secara khusus di ruang siber. Selain itu, koordinasi kelembagaan yang terfragmentasi antara BSSN, Kementerian Luar Negeri, Polri, dan TNI masih membatasi efektivitas penegakan hukum.

Pada tataran internasional, penelitian ini menemukan bahwa prinsip-prinsip inviolability dalam Konvensi Wina dapat diperluas ke ranah digital, mencakup arsip dan komunikasi elektronik. Namun, implementasinya terkendala oleh kesulitan atribusi, zona abu-abu spionase, serta reluktansi politik negara-negara untuk mengkonfrontasi aktor kuat. Penelitian ini menyimpulkan bahwa kerangka hukum Indonesia saat ini memberikan perlindungan yang parsial namun belum komprehensif. Oleh karena itu, disarankan adanya revisi peraturan nasional untuk secara eksplisit memasukkan misi diplomatik sebagai infrastruktur siber vital, pembentukan Standar Operasional Prosedur (SOP) khusus bagi insiden siber yang melibatkan kedutaan, serta peningkatan kerja sama di

---

[3] Student at the Department of International Law, Faculty of Law, Universitas Gadjah Mada (International Undergraduate Program 2021).
[4] Lecturer at the Department of International Law, Faculty of Law, Universitas Gadjah Mada.

tingkat ASEAN dan PBB guna memperkuat perlindungan entitas diplomatik di dunia maya.

Kata Kunci: Perang Siber, Kekebalan Diplomatik, Konvensi Wina, Hukum Indonesia, Spionase Siber, BSSN, Prinsip Inviolability.