ASHA PUBLISHING

BUSINESS REGULATION AND INTEGRITY LAW



Volume 1, Number 3, 2026

Business Regulation and Integrity Law
E-ISSN: 3124-2936
DOI: https://doi.org/10.70188/x3yggk78

Digital Diplomacy of Indonesia in Facing Global Cybersecurity Challenges

Muhammad Alim Arhas[1], Irsyad Dahri[2]
[1,2] Universitas Negeri Makassar
Email: alimarhas123@gmail.com

ABSTRACT

Digital diplomacy has emerged as a significant component of contemporary international relations, particularly through the use of information and communication technologies to facilitate diplomatic engagement and promote cooperation among countries. Advances in digital technology have gradually reshaped traditional diplomatic practices by introducing new forms of communication, transnational digital networks, and technology-driven governance. This study examines how Indonesia employs digital diplomacy to address global cybersecurity challenges through a literature-based approach. A descriptive qualitative design was employed using library research involving scholarly articles, academic books, official government publications, international reports, and relevant legal documents on digital diplomacy, cybersecurity, and data protection. The findings indicate that Indonesia's digital diplomacy extends beyond its conventional role as a channel of foreign policy communication. It also serves as a strategic instrument for strengthening international cybersecurity cooperation, advancing digital governance, and safeguarding national interests in cyberspace. Within the context of business law, cybersecurity issues are particularly associated with personal data protection, digital sovereignty, and the establishment of legal frameworks governing activities in the digital environment. The study further identifies the importance of integrating international collaboration, technological advancement, human resource capabilities, and responsive legal frameworks to support effective digital diplomacy. Strengthening these interconnected aspects is essential for enabling Indonesia to address evolving global cybersecurity challenges while protecting digital rights and national interests.

Keywords: digital diplomacy, cybersecurity, international relations, indonesia, cyber diplomacy

INTRODUCTION

Rapid advances in information and communication technologies (ICT), together with accelerating globalization, have reshaped various dimensions of human activity, including relations among states. These technological developments have transformed not only communication among individuals and societies but also the ways in which governments engage with other countries and pursue diplomatic objectives. Diplomatic practices, which traditionally relied on direct meetings, confidential negotiations, and established formal channels, are increasingly conducted through digital environments and technological platforms.

Digital environments have created new possibilities for states to communicate more rapidly, articulate their national interests, influence public perceptions at the international level, and engage with a broader range of global actors. This shift has contributed to the evolution of diplomatic practices and given rise to what is commonly known as digital diplomacy or e-diplomacy. The concept refers to the use of internet-based technologies and

digital communication channels by governments and diplomatic institutions to pursue and support foreign policy objectives.

Melissen (2015) describes digital diplomacy as an extension of public diplomacy that incorporates digital technologies to facilitate communication, distribute information, and develop wider connections between states and international audiences. The growing use of digital platforms has also expanded diplomatic engagement beyond conventional government-to-government relations, allowing international organizations, private sector actors, civil society groups, and global communities to participate more actively in diplomatic interactions.

For developing countries, including Indonesia, the growing use of digital diplomacy creates opportunities to strengthen their presence and engagement in international affairs. The use of digital technologies can reduce some constraints associated with traditional diplomatic practices by expanding channels for cross-border communication and cooperation. By making use of these digital channels, Indonesia is able to articulate its national interests, develop stronger relationships with international partners, and contribute to global dialogue concerning various strategic issues.

Cybersecurity has become a critical concern within the broader field of digital diplomacy. As digital technologies continue to advance and become increasingly integrated into global activities, countries face a growing range of cyber risks, such as attacks that extend across national borders, unauthorized exposure of sensitive data, and cybercrime involving actors from multiple jurisdictions. The transnational nature of these risks has expanded the scope of cybersecurity beyond technical and national security concerns, making it an increasingly important issue in contemporary international relations.

Because cyber threats frequently transcend national boundaries, addressing them requires coordinated action among countries rather than relying solely on individual state responses. Diplomatic engagement therefore plays an important role in facilitating the sharing of relevant information, developing stronger cybersecurity capabilities, and promoting common international standards for responsible conduct in cyberspace.

Within this setting, digital diplomacy serves as a relevant means for Indonesia to address cybersecurity issues that extend beyond national boundaries. Its application enables Indonesia to deepen cooperation with individual countries and multilateral partners, participate more actively in international cybersecurity dialogues, and contribute to shaping digital governance practices that promote security and responsible conduct in cyberspace.

Despite the growing academic attention given to digital diplomacy and cybersecurity, further examination is still needed to understand how Indonesia employs digital diplomacy in dealing with cybersecurity challenges at the global level. Existing research has largely addressed cybersecurity from a technological perspective or examined digital diplomacy primarily in terms of its communication role. Less attention has been directed toward the connection between diplomatic engagement in digital spaces, international collaboration on cybersecurity, and Indonesia's strategic position as a developing country. This gap highlights the need for a more comprehensive analysis of how these dimensions interact within Indonesia's response to contemporary cybersecurity issues.

Accordingly, this study examines Indonesia's use of digital diplomacy in addressing cybersecurity challenges at the global level, with particular attention to its contribution to strengthening the country's engagement and position within contemporary international relations.

A comprehensive examination of digital diplomacy requires an understanding of fundamental concepts in international relations, particularly changes in diplomatic practices, emerging security challenges, and state participation in global governance. Advances in digital technology have reshaped the international landscape, moving diplomatic interaction beyond

the traditional state-centered model that largely depended on conventional channels. Contemporary international relations operate within an increasingly complex setting in which multiple actors interact through digital environments. Diplomatic engagement is therefore no longer conducted exclusively through official representatives, bilateral encounters, and participation in formal international forums. Governments increasingly rely on digital platforms to facilitate communication and negotiation, reach wider audiences, and articulate their national interests more rapidly.

This transformation illustrates the growing importance of digital technology in supporting states' efforts to achieve their foreign policy objectives. As international relations become more interconnected, technological capabilities are increasingly associated not only with digital advancement but also with the ability of states to extend their influence, safeguard national security, and contribute to the formation of global governance. Digital diplomacy therefore provides an important conceptual framework for examining the ways in which technology is incorporated into diplomatic practices. At the same time, cybersecurity offers a relevant perspective for understanding the emerging risks and security concerns arising from states' growing reliance on digital systems.

The position of developing countries also deserves particular attention in discussions of digital diplomacy. The expansion of digital technologies has opened new avenues for these countries to become more actively involved in international affairs by taking advantage of digital platforms and networks. For Indonesia, digital diplomacy may serve as a strategic approach for enhancing cooperation with international partners, responding to emerging cybersecurity concerns, and broadening its involvement in global digital governance. Accordingly, this study draws on digital diplomacy, cybersecurity, and the position of developing countries as its principal conceptual foundations for examining Indonesia's use of technology in advancing national interests within an increasingly digital international environment.

Digital Diplomacy Concept

The rapid advancement of information and communication technologies has contributed to significant changes in conventional diplomatic practices, leading to the growing prominence of digital diplomacy. Melissen (2015) describes digital diplomacy as the use of internet-based technologies by foreign ministries and other diplomatic actors to pursue foreign policy objectives. Within this context, digital diplomacy can be viewed as an expansion of public diplomacy that provides states with new channels for engaging directly with international audiences. These channels enable governments to disseminate information, promote their national image, and establish broader networks within the international community.

Traditional diplomacy has generally depended on formal interactions and negotiations among official state representatives, whereas digital diplomacy extends these activities into online environments. The use of digital platforms enables governments to engage with a wider range of actors, including international communities, global organizations, private sector institutions, and civil society groups. Bjola and Holmes (2015) emphasize that the incorporation of digital technologies into foreign policy practices has reshaped the ways in which diplomatic communication is conducted.

From this perspective, the role of digital diplomacy extends beyond facilitating communication and increasingly forms part of broader strategies for advancing national interests. Governments can employ digital platforms to deepen cooperation with international partners, shape how their policies and interests are perceived globally, and engage in international dialogue on newly developing issues, particularly those concerning cybersecurity and the governance of digital environments.

Cybersecurity in International Relations

Cybersecurity is no longer viewed solely as a technical issue involving the protection of information systems; it has increasingly become a strategic concern in international relations. Growing state reliance on digital infrastructure has also introduced various forms of vulnerability, particularly those arising from cyberattacks, unauthorized access to sensitive data, and criminal activities conducted through digital networks.

Kello (2017) identifies cyberspace as an increasingly significant domain of international security, given that activities conducted within it may have consequences for political stability, economic processes, and state sovereignty. Cyber threats differ from many traditional security challenges because they are not confined by territorial boundaries and may involve a diverse range of actors, including governments, private entities, and other non-state actors.

Schmitt (2017) highlights the importance of international collaboration in addressing cybersecurity concerns, particularly through the formulation of norms that guide responsible state conduct in cyberspace. Given the transnational nature of many cyber threats, individual state responses are often insufficient. Diplomatic channels therefore become important for facilitating information sharing, coordinating cooperative measures among countries, and developing international arrangements for the governance of cybersecurity.

Digital Governance, Data Protection, and Business Law Perspective

The continued expansion of digital activities has raised various legal concerns, particularly regarding personal data protection, privacy, and transactions conducted through digital platforms. Within the field of business law, cybersecurity has therefore become increasingly relevant to safeguarding personal information, protecting consumer rights, and ensuring legal certainty for individuals and organizations operating in digital environments.

The growing reliance on digital platforms across economic and governmental sectors has increased the need for regulatory mechanisms that can respond to various digital risks, including the misuse of data, unlawful access to information, and cybercrime. In the Indonesian context, the adoption of Law Number 27 of 2022 on Personal Data Protection marks a significant development in establishing stronger legal safeguards for personal data amid the continuing expansion of digital activities.

The governance of digital environments depends on aligning technological advancement with appropriate legal frameworks. Managing cybersecurity effectively involves more than the application of technical measures, as it also depends on adequate legal mechanisms, coordination among relevant institutions, and collaboration across national borders. Digital diplomacy is therefore significant not only within the sphere of international relations but also in supporting the formulation and development of legal arrangements that regulate activities and interactions in cyberspace.

The Role of Developing Countries in Digital Diplomacy

The continuing shift toward digitalization has opened wider opportunities for developing countries to strengthen their involvement in international affairs. Nye (2011) suggests that technological capabilities can contribute to a state's capacity to exercise influence internationally, particularly when they are utilized as part of its soft power resources.

For developing states such as Indonesia, the use of digital diplomacy can help reduce some of the constraints associated with traditional diplomatic practices by widening access to international communication networks and collaborative initiatives. Indonesia's involvement in global digital governance also creates opportunities to participate more actively in international deliberations concerning cybersecurity, the governance of the internet, and the formulation of regulatory arrangements for the digital sphere.

Indonesia's strategic presence in Southeast Asia, together with the continued expansion of its digital ecosystem, provides a foundation for greater involvement in the development of cybersecurity cooperation at both regional and international levels.

METHODS

This study adopts a descriptive qualitative design based on library research to examine Indonesia's use of digital diplomacy in addressing global cybersecurity challenges. A qualitative design is appropriate because the analysis focuses on interpreting and explaining the phenomenon rather than statistically examining relationships among variables. The study therefore draws on relevant concepts, policy materials, documentary sources, and previous scholarly works to examine digital diplomacy and cybersecurity within the broader framework of international relations.

The descriptive method is applied to examine the ways in which Indonesia employs digital diplomacy to foster cooperation with international partners, deal with cybersecurity risks, and enhance its involvement in global digital governance. Using this method, the research explores how advances in digital technology are connected to the evolving nature of diplomatic practices and the strategies adopted by states to manage new forms of security threats arising in cyberspace.

Library research was considered appropriate for this study because the issues under examination involve public policies, diplomatic practices, and global developments that are extensively documented in written materials. Drawing on diverse sources allows the research to develop a broader interpretation of Indonesia's digital diplomacy by reviewing relevant scholarly literature, policy documents, and institutional reports. This method also makes it possible to consider different perspectives on the growing significance of digital technology in international relations rather than relying on a single type or source of data.

The analysis is organized around three central dimensions. These include Indonesia's use of digital diplomacy to promote cooperation with international partners, its application in responding to cybersecurity concerns, and the opportunities and constraints associated with Indonesia's position as a developing country within global digital governance. Together, these dimensions provide the analytical basis for examining how Indonesia incorporates digital technology into its efforts to pursue and protect national interests.

The research involved several stages, beginning with the identification and collection of relevant materials, followed by the selection of literature based on its relevance to the research focus. The selected materials were then examined to identify pertinent information, which subsequently formed the basis for interpreting the findings. This procedure was intended to produce a structured account of how Indonesia employs digital diplomacy in responding to cybersecurity challenges within the global environment.

Data Sources

The analysis relies on secondary data drawn from a range of sources that correspond to the subject of the study. Such data are considered suitable because the research examines established concepts, policy developments, diplomatic practices, and cybersecurity issues that have previously been recorded and discussed in written materials. The sources consisted of scholarly journal articles, academic books, official government publications on Indonesia's foreign policy and cybersecurity, reports issued by international organizations and cybersecurity research institutions, and relevant information published by credible media outlets.

Scholarly literature, particularly journal articles and academic books, provides the theoretical and conceptual basis for examining digital diplomacy, cybersecurity, international politics, and the position of developing countries within global digital governance. Official government publications are examined to identify Indonesia's policy direction and strategic initiatives for promoting international collaboration in digital technology and cybersecurity. Materials issued by international organizations and research institutions complement these sources by providing information on evolving cyber threats, patterns of cooperation among countries, and the difficulties states encounter as the global digital environment continues to change.

Sources were selected by considering their relevance to the research objectives, their direct relationship with digital diplomacy and cybersecurity, the credibility of the materials, and the currency of the information presented. The literature and documents that met these considerations were subsequently organized into thematic categories. These categories covered the evolution of Indonesia's digital diplomacy, approaches to bilateral and multilateral cooperation, initiatives undertaken to respond to cybersecurity risks, and Indonesia's participation as a developing country in the broader framework of international digital governance.

Information gathered from the selected sources was examined to understand the ways in which digital diplomacy is incorporated into Indonesia's foreign policy, the country's involvement in international efforts concerning cybersecurity, and the conditions that facilitate or constrain its diplomatic response to cyber threats extending across national boundaries.

Data Collection Technique

Data were collected through a review of literature and documentary materials relevant to the research topic. In accordance with the library research design, written sources were systematically identified and selected based on their relevance to the research objectives. The information derived from these materials was then used to examine Indonesia's application of digital diplomacy in responding to cybersecurity challenges at the global level.

The collection process initially focused on locating materials that corresponded with the main themes of the study, particularly digital diplomacy, cybersecurity within international relations, technological cooperation among countries, and the participation of developing states in global digital governance. Once the relevant materials had been gathered, they were screened according to their connection with the research objectives and the reliability of their sources. This process ensured that only appropriate and credible literature and documents were included in the analysis.

The materials that passed the selection stage were subsequently reviewed in greater detail, with relevant information recorded and organized according to the major themes of the study. The classification process covered several areas of analysis, namely Indonesia's approaches to digital diplomacy, cybersecurity collaboration through bilateral and multilateral arrangements, policies concerning data protection and digital security, and the various constraints encountered in the implementation of digital diplomacy.

This process provided a broad range of information on the evolution of Indonesia's digital diplomacy and its application in responding to changing cybersecurity issues at the global level. The information gathered from the selected sources was subsequently used as the basis for further analysis and interpretation of the position and function of Indonesia's digital diplomacy within contemporary international relations.

Data Analysis Technique

Content analysis was used to examine data obtained from the selected materials. This analytical technique enabled relevant information from different sources to be systematically

identified, interpreted, and organized in accordance with the research focus. Its use was considered appropriate because the study primarily draws upon documentary materials, scholarly literature, and other written sources discussing Indonesia's digital diplomacy and cybersecurity issues at the global level.

The analysis involved several stages, beginning with the identification of information relevant to the study's objectives. During this initial stage, the available materials were reviewed and relevant data were extracted concerning digital diplomacy as a concept, Indonesia's approaches to strengthening cooperation with international partners, emerging cybersecurity threats, and policy developments within the field of digital governance.

In the second stage, the information identified from the selected sources was organized according to the principal themes of the study. The data were grouped into several analytical areas covering the incorporation of digital diplomacy into Indonesia's foreign policy, cybersecurity collaboration at bilateral and multilateral levels, measures undertaken to safeguard data and digital infrastructure, and the constraints encountered by Indonesia in carrying out its digital diplomacy initiatives.

The third stage focused on interpreting the information through comparison across the selected materials. Scholarly perspectives were examined alongside policy documents and relevant institutional reports to develop a broader understanding of Indonesia's position and strategic responses to evolving cybersecurity issues at the global level. The results of this comparison were subsequently integrated to identify recurring patterns, connections among the findings, and key interpretations that corresponded with the objectives of the research.

The final stage consisted of formulating conclusions from the results of the preceding analysis. These conclusions were developed by examining the interconnections among advances in digital technology, Indonesia's national interests, the practice of digital diplomacy, and patterns of international cooperation aimed at strengthening cybersecurity.

Through this analytical framework, the research aims to develop a structured understanding of how Indonesia employs digital diplomacy in responding to cybersecurity challenges that extend across national boundaries. Digital technology is examined not simply as a medium for diplomatic interaction, but as part of a broader strategic approach that facilitates cooperation among countries, contributes to the formulation of norms for the digital environment, and supports Indonesia's participation in the governance of global cyberspace.

RESULT AND DISCUSSION

Indonesia's approach to cybersecurity-related digital diplomacy can be examined through several dimensions, including the use of digital capabilities to promote international cooperation, safeguard national interests, and address increasingly sophisticated cyber risks. Technological advances have significantly altered the nature and scope of security threats, as cyber incidents are not confined to national borders and may involve actors operating from different jurisdictions. The transnational nature of these threats has made cybersecurity a shared global concern that cannot be addressed effectively by individual states alone and requires coordinated international action.

The evolving character of cyber threats has contributed to a broader transformation in contemporary diplomatic practices. Diplomacy now extends beyond formal channels of communication among states and increasingly serves as a mechanism for coordinating responses, sharing relevant information, strengthening institutional capabilities, and developing common norms for activities in cyberspace. Digital diplomacy enables governments to take advantage of technological platforms to broaden international partnerships, articulate national priorities, and become more actively involved in the formation of global digital governance.

Indonesia's engagement in cybersecurity diplomacy reflects an adjustment of its international relations practices to the evolving global strategic landscape. Growing reliance on digital technologies creates a dual imperative for Indonesia as a developing country: enhancing domestic cybersecurity capabilities and maintaining active engagement with international partners. Within this context, Indonesia's approach can be examined through several key dimensions, particularly its efforts to expand bilateral and multilateral collaboration, manage concerns surrounding data sovereignty and the security of public institutions, and overcome constraints affecting the implementation of digital diplomacy.

Strengthening Multilateral and Bilateral Cooperation

Indonesia has sought to address cybersecurity concerns through digital diplomacy by increasing its participation in international discussions and cooperation forums. This includes engagement in United Nations processes concerned with security in the use of information and communication technologies, particularly the Open-Ended Working Group (OEWG). Such participation reflects Indonesia's recognition that cybersecurity extends beyond technical considerations and increasingly intersects with political, economic, and security interests within contemporary international relations.

Indonesia uses international forums to promote a digital environment that balances security, openness, and inclusivity while taking into account the interests of countries at different stages of development. Its participation also reflects an effort to move beyond the role of a technology user by contributing to discussions on the norms and regulatory principles that shape state conduct in cyberspace. This involvement has become increasingly relevant as technological connectivity deepens interdependence among countries, making national digital security closely linked to cybersecurity conditions beyond a state's own borders.

Indonesia's involvement in multilateral forums illustrates the broader transformation taking place in contemporary diplomacy. Diplomatic engagement that once depended largely on face-to-face interaction among official representatives and formal negotiation procedures can now also be conducted through digitally mediated channels. Virtual conferences, electronic exchanges of diplomatic materials, and online coordination networks have become part of this evolving practice. For Indonesia, these mechanisms create more flexible opportunities to engage with international agendas and broaden its participation in global deliberations concerning cybersecurity.

Integrating technology into Indonesia's diplomatic activities has expanded the channels through which the country can communicate its national interests to international audiences and partners. Digital diplomacy allows diplomatic communication to continue beyond scheduled meetings and formal international forums through a variety of online interactions. These expanded channels can support Indonesia in building wider cooperative networks, maintaining strategic engagement with external partners, and contributing more actively to international discussions concerning the formulation of cybersecurity policies.

Beyond its participation in multilateral initiatives, Indonesia also develops cybersecurity partnerships with individual strategic partners through bilateral cooperation. Such arrangements are particularly important because countries differ in their technological resources, institutional experience, and capacity to manage cyber risks. Bilateral engagement therefore provides Indonesia with opportunities to share information on emerging cyber threats, strengthen the expertise of its human resources, enhance technical capabilities, and improve the institutional capacity of agencies responsible for digital security.

Indonesia has also sought to strengthen its domestic cybersecurity capabilities by developing partnerships with countries such as Japan and the United States, as well as with members of the European Union, allowing knowledge and experience to be shared across national boundaries. The scope of these partnerships extends beyond technical cooperation to include the formulation of relevant policies, the strengthening of institutional capacities, and the development of coordination arrangements for responding to increasingly sophisticated cyber threats.

For developing states, bilateral partnerships in cybersecurity can play an important role in addressing gaps in technological resources and domestic capabilities. International collaboration gives Indonesia opportunities to draw on external expertise, technological knowledge, and established practices for managing digital security. In this sense, digital diplomacy extends beyond its function as a channel of political interaction and becomes a mechanism through which national cybersecurity capacity can be strengthened in response to security challenges with an increasingly global character.

The expansion of Indonesia's bilateral and multilateral partnerships highlights two interconnected roles of digital diplomacy in the cybersecurity field. One relates to the advancement of national interests through Indonesia's involvement in the development of global cybersecurity governance. The other concerns the strengthening of domestic capacity by drawing on cooperation, expertise, and resources available through international partnerships. Together, these roles indicate that digital diplomacy is becoming increasingly relevant to Indonesia's efforts to adapt its security strategies to the evolving international environment shaped by digital transformation.

Response to Data Sovereignty and Public Sector Security Issues

The increasing exposure of public institutions to cyber threats has reinforced the importance of data protection as an element of state sovereignty in the digital age. Government-held data, public information systems, and national digital infrastructure now carry strategic importance because their operation is closely tied to the delivery of public services, the continuity of governmental functions, economic stability, and national security. Protecting these assets therefore requires more than technical cybersecurity measures; it is also fundamental to preserving state authority and sovereignty in cyberspace.

As government activities become increasingly dependent on digital technologies, public institutions are exposed to a wider range of risks, such as the disclosure of sensitive data, unlawful access to information systems, attacks against digital infrastructure, and interruptions to digitally delivered public services. Cybersecurity threats differ from traditional security concerns because they are not necessarily confined by territorial borders and may originate from diverse actors with varying levels of capability. Protecting national data therefore requires an integrated approach that extends beyond security measures implemented solely within domestic institutions.

Indonesia has increasingly incorporated digital diplomacy into its response to these challenges by developing partnerships with international actors that have relevant expertise and advanced capabilities in cybersecurity. The transnational nature of digital threats makes such collaboration particularly important, as effective responses often depend on cross-border information sharing, technical coordination, and common approaches among participating countries. These diplomatic partnerships provide Indonesia with opportunities to enhance cooperation in information security, learn from established cybersecurity practices, and further develop its domestic capacity to manage emerging digital risks.

Cybersecurity cooperation with international partners can also support Indonesia in enhancing its capacity to identify emerging threats, secure critical digital infrastructure, and establish more effective mechanisms for handling cyber incidents. As cyber risks continue to

change in form and complexity, sharing knowledge about attack patterns, security technologies, and appropriate mitigation measures becomes increasingly valuable. Such collaboration therefore extends beyond responding to incidents that have already occurred and also contributes to preventive efforts aimed at developing more resilient cybersecurity systems.

At the domestic level, the National Cyber and Crypto Agency (BSSN) plays an important role in coordinating Indonesia's cybersecurity efforts. Its responsibilities include enhancing the security of information systems, improving human resource capabilities, contributing to the formulation of cybersecurity strategies, and facilitating coordination among stakeholders in responding to digital risks. The scope of these responsibilities illustrates that effective cybersecurity cannot depend on a single institution, but requires participation from government agencies, private sector organizations, educational institutions, and international partners.

International partnerships facilitated through digital diplomacy can contribute to Indonesia's cybersecurity development by enhancing technical expertise, reinforcing institutional capabilities, and supporting the formulation of strategies for managing increasingly sophisticated cyber risks. These contributions illustrate how the international and domestic dimensions of cybersecurity are closely interconnected. Digital diplomacy therefore extends beyond maintaining relationships with foreign partners, as the knowledge, experience, and cooperation generated through such engagement can also support the strengthening of Indonesia's internal cybersecurity capacity.

Digital diplomacy concerning data security therefore has implications that extend beyond Indonesia's engagement with external partners, as it also contributes to the development of domestic cybersecurity capabilities. The capacity to safeguard the national digital environment is essential for maintaining confidence among international partners, preserving the continuity of technology-based public services, and enabling technological advancement to contribute to the long-term pursuit of national interests.

Challenges of Indonesia's Digital Diplomacy Implementation

Despite the opportunities created by digital diplomacy for broader Indonesian participation in international affairs, several constraints continue to affect its implementation. The success of this form of diplomacy depends on more than access to digital technologies. Institutional preparedness, qualified personnel, appropriate regulatory arrangements, and the strategic management of communication are equally important in determining how effectively digital diplomacy can be conducted.

A major constraint concerns disparities in digital infrastructure and technological readiness across government institutions. Variations in the quality of information systems and institutional digital capabilities may hinder coordination and the timely exchange of information required for diplomatic activities. An integrated technological environment is particularly important in cybersecurity, where government agencies must be able to communicate and coordinate rapidly as threats emerge and evolve.

The importance of infrastructure becomes more apparent when dealing with cyber incidents that demand immediate and coordinated action. Insufficient technological capacity can weaken the ability of institutions to identify potential threats, exchange security information, and manage appropriate responses. Improving the reliability and integration of digital infrastructure is therefore fundamental to strengthening both cybersecurity management and the implementation of Indonesia's digital diplomacy.

Human resource capacity is another area that requires attention. Contemporary digital diplomacy demands competencies that combine an understanding of diplomatic affairs with knowledge of cybersecurity, information systems, technology governance, and other digital

issues. As technological matters become increasingly prominent on the international agenda, diplomats and policymakers need sufficient digital literacy to interpret cybersecurity developments and engage meaningfully in international negotiations and discussions.

Developing these competencies is therefore an important part of Indonesia's digital diplomacy agenda. Professional education, specialized training, and opportunities for knowledge exchange with international partners can contribute to stronger expertise in dealing with global cybersecurity matters. Technological progress by itself offers limited benefits when the individuals responsible for policy and diplomacy lack the capabilities required to understand and manage complex digital risks.

Additional challenges arise from the characteristics of online information environments, particularly the spread of misinformation, disinformation, and digital propaganda. Information distributed through digital platforms can spread rapidly across national borders and potentially shape public opinion as well as perceptions of a country internationally. Managing digital diplomacy therefore requires both technical competence and carefully designed communication practices capable of presenting national policies and interests clearly and accurately.

The circulation of misleading or inaccurate information further illustrates the close relationship between cybersecurity and information governance. Protecting the digital environment must be accompanied by efforts to maintain reliable communication with audiences inside and outside the country. Achieving this requires coordination involving government agencies, technology companies, academic institutions, and wider society.

Legal preparedness represents an additional challenge from a business law perspective. Continuous technological innovation generates legal questions concerning the protection of personal information, electronic transactions, privacy, and responsibility for activities conducted in cyberspace. Legal arrangements supporting digital diplomacy must therefore be capable of adapting to technological change while providing adequate protection and certainty for actors operating within digital environments.

For Indonesia, the development and implementation of appropriate legal frameworks are consequently integral to broader cybersecurity efforts. Rules governing personal data, electronic transactions, and digital governance provide an important legal basis for ensuring that the expansion of technology takes place in accordance with legal principles while respecting and protecting individual rights.

Responding to these interconnected challenges calls for an approach that combines technological capability, regulatory development, institutional coordination, and sustained investment in human resources. Indonesia's digital diplomacy is likely to function more effectively when international engagement is reinforced by strong domestic institutional and legal foundations. Strengthening these areas can enhance Indonesia's participation in global digital governance while improving its capacity to respond to the changing nature of cybersecurity challenges.

CONCLUSION

Digital diplomacy has evolved beyond its initial function as an additional communication channel and now plays a more strategic role in contemporary international relations. Advances in information and communication technologies have reshaped diplomatic interaction, allowing governments to engage with global audiences and pursue national priorities through new forms of communication. Its significance is particularly evident in cybersecurity, where threats frequently transcend territorial boundaries and consequently require responses that extend beyond measures undertaken at the domestic level.

The findings indicate that Indonesia's digital diplomacy strengthens its participation in international cybersecurity initiatives and facilitates cross-border cooperation. Participation in multilateral mechanisms, together with bilateral partnerships, provides Indonesia with channels to articulate national priorities, enhance cybersecurity capabilities, share relevant information with foreign partners, and take part in discussions concerning the development of a more secure and responsible global digital environment.

Indonesia's experience further illustrates the changing position of technology within contemporary diplomacy. Rather than functioning only as a medium for communication, digital technology has become integrated into state strategies for expanding international engagement, developing cooperative relationships, and participating in the governance of global digital affairs. This development is especially relevant for Indonesia as a developing country because digital channels can broaden access to international networks, reduce some constraints associated with conventional diplomatic practices, and create greater opportunities to engage in international debates on cybersecurity and digital regulation.

Nevertheless, the benefits of international engagement depend largely on the strength of Indonesia's domestic capabilities. Adequate digital infrastructure, competent human resources, responsive cybersecurity regulation, effective personal data protection, and stronger coordination across relevant institutions constitute important foundations for the implementation of digital diplomacy. International cooperation is therefore most meaningful when accompanied by sufficient institutional, technological, and regulatory capacity at the national level.

From a Business Law perspective, these developments also emphasize the growing relationship between diplomatic engagement, technological change, and legal governance. The expansion of activities in cyberspace creates a continuing need for legal arrangements capable of addressing cybersecurity risks, safeguarding personal data, and governing digital activities while providing legal certainty. Such arrangements are also important for balancing the protection of individual rights with the preservation of national interests in the digital sphere.

Digital diplomacy therefore represents an increasingly important component of Indonesia's efforts to pursue national interests amid ongoing digital transformation. Greater integration of technological capabilities, international partnerships, domestic institutional capacity, and responsive legal regulation can strengthen Indonesia's engagement with global cybersecurity issues. These interconnected efforts can also support Indonesia's contribution to the establishment of a digital environment characterized by greater security, responsibility, and long-term sustainability.

REFERENCES

Bjola, C., & Holmes, M. (Eds.). (2015). *Digital diplomacy: Theory and practice*. Routledge. https://www.routledge.com/Digital-Diplomacy-Theory-andPractice/Bjola-Holmes/p/book/9781138843820

Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press. https://mitpress.mit.edu/9780262517690/cyberpolitics-in-international-relations/

Hocking, B., & Melissen, J. (2015). *Diplomacy in the digital age*. Netherlands Institute of International Relations Clingendael. https://www.clingendael.org/publication/diplomacy-digital-age-0

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press. https://doi.org/10.12987/9780300226294

Manor, I. (2019). *The digitalization of public diplomacy*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-04405-3

Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.

Republic of Indonesia. (2008). *Law of the Republic of Indonesia Number 11 of 2008 concerning electronic information and transactions*.

Republic of Indonesia. (2022). *Law of the Republic of Indonesia Number 27 of 2022 concerning personal data protection*.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

United Nations. (2025). *Final report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025* (A/80/257). https://meetings.unoda.org/meeting/57871/documents

World Bank. (2016). *World development report 2016: Digital dividends*. World Bank.

World Bank. (2021). *World development report 2021: Data for better lives*. World Bank. https://doi.org/10.1596/978-1-4648-1600-0