JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882

http://journals.academiczone.net/index.php/jiphr

Digital Diplomacy and Cybersecurity: Protecting Diplomatic Communications in the Digital Age

Yuldasheva Govkherjan

Doctor of Science in Law, Professor of the Department of International law and human rights, Tashkent State University of Law, Uzbekistan

Abstract: The rapid digitalization of diplomatic communications has fundamentally transformed how states conduct foreign policy, negotiate treaties, and manage international relations. While digital technologies have enhanced the speed, efficiency, and reach of diplomatic engagement, they have simultaneously exposed governmental actors to unprecedented cybersecurity threats. This article examines the intersection of digital diplomacy and cybersecurity, analyzing the evolving threat landscape facing diplomatic missions, foreign ministries, and international organizations. Drawing on case studies of major cyberattacks targeting diplomatic infrastructure, including the 2016 U.S. Democratic National Committee breach, the 2020 SolarWinds campaign, and persistent intrusions against European Union diplomatic networks, the paper identifies systemic vulnerabilities in diplomatic communications systems. The article further evaluates existing international legal frameworks, including the Vienna Convention on Diplomatic Relations, for their adequacy in addressing cyber threats to diplomatic communications. It proposes a multilayered security architecture encompassing end-to-end encryption, zero-trust network models, diplomatic cyber norms, and capacity-building programs for developing nations. The findings suggest that protecting diplomatic communications requires a holistic approach integrating technological safeguards, legal innovations, and multilateral cooperation frameworks that transcend existing bilateral arrangements. The article concludes with policy recommendations for foreign ministries, international organizations, and cybersecurity practitioners seeking to strengthen the resilience of diplomatic communications infrastructure in an increasingly contested digital environment.

Keywords: digital diplomacy, cybersecurity, diplomatic communications, cyber threats, e-diplomacy, international relations, cyber norms, information security, foreign policy, encryption

Introduction

The advent of digital technology has profoundly reshaped the practice of diplomacy. Foreign ministries, ambassadors, and international negotiators now rely on email, secure messaging applications, video conferencing platforms, and cloud-based information systems to conduct the day-to-day business of statecraft. This transition from paper-based, courier-reliant communication to instantaneous digital exchange has accelerated diplomatic processes, broadened participation in international forums, and enabled the rise of what scholars have termed 'digital diplomacy' or 'e-diplomacy' (Bjola & Holmes, 2015). Yet these same technologies have introduced vulnerabilities that adversaries state and non-state alikeare determined to exploit.

The protection of diplomatic communications has historically been regarded as a cornerstone of international relations. The Vienna Convention on Diplomatic Relations (1961) established inviolability of diplomatic bags, premises, and correspondence as foundational principles of the

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

international order. However, these protections were conceived in an era when sensitive communications traveled physically, sealed in pouches or locked in vaults. The emergence of cyber espionage, data exfiltration, and network intrusion has exposed a critical gap between the existing legal architecture and the realities of twenty-first-century diplomacy (Dinniss, 2012). Nation-state actors, criminal organizations, and hacktivist groups now routinely target diplomatic networks to intercept sensitive negotiations, steal intelligence, and undermine foreign policy objectives.

This article investigates the cybersecurity challenges confronting digital diplomacy and proposes a framework for protecting diplomatic communications in the digital age. Section two provides a conceptual foundation, defining digital diplomacy and situating it within broader cybersecurity discourse. Section three examines the evolving threat landscape, cataloguing the actors, vectors, and motivations behind cyberattacks on diplomatic infrastructure. Section four analyzes significant case studies of diplomatic cyber incidents to distill lessons for practitioners and policymakers. Section five evaluates the adequacy of international legal norms and proposes reforms. Section six advances a multilayered technical and institutional security framework. Section seven discusses implications for emerging economies and diplomatic capacity building, and section eight concludes with policy recommendations.

Defining Digital Diplomacy. Digital diplomacy, variously described as e-diplomacy, cyber diplomacy, or tech diplomacy, encompasses the use of information and communications technology (ICT) by state and non-state actors to pursue foreign policy objectives (Hocking & Melissen, 2015). Scholars distinguish between two dimensions of the concept. The first is the use of digital tools social media platforms, encrypted messaging, data analytics, and virtual conferencing as instruments for conducting traditional diplomatic activities such as negotiation, signaling, and public diplomacy. The second dimension involves diplomacy about the digital domain itself: the negotiation of international norms, treaties, and governance frameworks governing cyberspace, artificial intelligence, and emerging technologies (Mueller, 2017).

The practical manifestations of digital diplomacy are wide-ranging. Foreign ministries deploy social media strategies to shape international narratives and engage diaspora communities. Heads of state conduct virtual summits that transcend geographical constraints. Intelligence services leverage open-source data analytics to monitor geopolitical developments in real time. The United Nations and regional organizations rely on cloud-based platforms to coordinate humanitarian operations across conflict zones. Each of these activities generates sensitive data flows that must be secured against unauthorized access (Bjola & Zeng, 2017).

Cybersecurity in the Diplomatic Context. Cybersecurity, defined broadly as the protection of information systems and the data they contain from unauthorized access, disruption, or destruction, is particularly consequential in diplomatic settings because of the sensitivity of the information at stake (Kosseff, 2018). Diplomatic communications routinely include classified intelligence assessments, negotiating positions, personnel information, and strategic plans. Compromise of such information can jeopardize ongoing negotiations, endanger human sources, trigger diplomatic incidents, and provide adversaries with decisive strategic advantage.

The Central Intelligence Agency's triad model confidentiality, integrity, and availability provides a useful framework for analyzing cybersecurity risks to diplomatic systems. Confidentiality breaches allow adversaries to read sensitive communications; integrity attacks allow them to alter or fabricate messages; and availability attacks disable communications infrastructure at critical moments (Stallings & Brown, 2018). All three dimensions are implicated in cyber operations targeting diplomatic actors, and each demands distinct technical and procedural countermeasures.

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

State-Sponsored Cyber Espionage. The most significant and persistent cybersecurity threat to diplomatic communications emanates from state-sponsored actors. Nation-states have long recognized that intelligence derived from intercepted diplomatic communications can yield enormous strategic dividends, from gaining advance knowledge of an adversary's negotiating red lines to identifying vulnerabilities in coalition relationships. The digitalization of diplomatic channels has dramatically reduced the cost and increased the scale of such intelligence collection (Rid, 2013). Advanced Persistent Threat (APT) groups attributed to Russia, China, Iran, and North Korea among others have been documented conducting sustained intrusion campaigns against foreign ministries, embassies, and international organizations across multiple continents.

Russia's Foreign Intelligence Service (SVR) and its affiliated APT29, also known as Cozy Bear, has demonstrated particular sophistication in targeting diplomatic networks. APT29 employs a distinctive operational pattern characterized by low-and-slow intrusion techniques, living-off-the-land tactics that minimize forensic footprints, and patient exploitation of trusted software supply chains (Mandiant, 2021). China's Ministry of State Security maintains numerous APT groups that have systematically targeted the diplomatic infrastructure of Southeast Asian states, European Union institutions, and African governments to support Belt and Road Initiative negotiations and monitor opposition movements (FireEye, 2020).

Insider Threats and Social Engineering. Beyond external intrusion, diplomatic missions face significant risks from insider threats and social engineering attacks. Diplomatic personnel constitute attractive targets for recruitment by foreign intelligence services, and the pressures of overseas postings financial strain, personal vulnerabilities, ideological disaffection create conditions amenable to exploitation (Gelles, 2016). High-profile cases including Robert Hanssen of the FBI and Ana Montes of the Defense Intelligence Agency illustrate the catastrophic damage that can result when insiders with access to sensitive communications systems are compromised.

Phishing and spear-phishing campaigns represent the most common initial vector for breaches of diplomatic networks (Verizon, 2022). Adversaries craft convincing emails impersonating trusted interlocutors heads of state, senior officials, international organization counterparts to induce targets to click malicious links or open weaponized attachments. Once initial access is established, attackers can move laterally through the network, escalate privileges, and exfiltrate data over extended periods without detection. The 2015 breach of the German Bundestag, attributed to APT28, began with a simple phishing email and ultimately resulted in the exfiltration of 16 gigabytes of parliamentary data (Sanger, 2018).

Technical Vulnerabilities in Diplomatic Infrastructure. Diplomatic networks often present attractive targets due to structural vulnerabilities that reflect institutional culture rather than technical inadequacy alone. Many foreign ministries maintain aging legacy systems that lack modern security controls and cannot easily accommodate encryption or multi-factor authentication. Diplomatic posts in developing countries frequently operate with limited cybersecurity staff, inadequate patch management processes, and insufficient network segmentation. Bring-your-own-device policies common in diplomatic settings where officials use personal smartphones for official communication create significant endpoint security risks (Oltsik, 2019).

The proliferation of third-party cloud services and communication applications has further complicated the security calculus for diplomatic organizations. While commercial platforms such as Microsoft Teams, Zoom, and WhatsApp offer convenience and interoperability, their use for sensitive diplomatic communications raises serious concerns about data sovereignty, encryption standards, and exposure to signals intelligence collection (Rid & Buchanan, 2015). Several European foreign ministries have

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

invested in sovereign communications infrastructure domestically developed encrypted messaging systems precisely to mitigate these risks.

The SolarWinds Supply Chain Attack (2020). The SolarWinds compromise, attributed by the United States government to the Russian SVR, represents one of the most consequential cyberattacks in the history of espionage and merits detailed examination for its implications regarding diplomatic communications security. Beginning in late 2019, Russian operatives inserted malicious code into the Orion network monitoring software produced by SolarWinds Corporation, a widely used IT management platform. When SolarWinds distributed routine software updates in spring 2020, approximately 18,000 organizations including the U.S. Department of State, Treasury, and multiple other federal agencies unwittingly installed the malicious backdoor (CISA, 2021). The attackers leveraged this access over a nine-month period to conduct highly targeted intelligence collection against selected high-value victims, including diplomatic and foreign policy infrastructure.

The SolarWinds case illuminates several critical lessons for diplomatic cybersecurity. First, supply chain vulnerabilities represent a fundamental challenge for which traditional perimeter-based security models are wholly inadequate. Trusted software vendors can serve as force multipliers for adversaries seeking to penetrate well-defended networks without triggering intrusion detection systems. Second, the extended dwell time months between initial compromise and detection—underscores the importance of behavioral analytics and anomaly detection capabilities that can identify malicious activity patterns even when the malware itself evades signature-based defenses. Third, the incident demonstrated the inadequacy of existing international norms in providing deterrence against sophisticated state-sponsored operations (Microsoft, 2021).

EU Diplomatic Network Breaches. The European Union's diplomatic communications network fell victim to a sustained intrusion campaign discovered in 2018 and 2019 by the cybersecurity firm Area 1 Security. Attackers subsequently attributed to PLA Unit 61398, a Chinese military cyber unit gained access to the EU's classified communications network, known as COREU, and systematically exfiltrated cables documenting sensitive diplomatic discussions about China-EU trade negotiations, the Iran nuclear deal, and Russian military activities in Ukraine (Area 1 Security, 2018). The breach exposed thousands of diplomatic cables spanning a three-year period and reportedly compromised European negotiating positions in several significant multilateral forums.

The EU incident highlights the particular vulnerability of shared multilateral communications networks to targeted intrusion. When multiple member states share a common communications platform, a single point of compromise can expose the confidential communications of dozens of governments simultaneously. The incident also demonstrated the critical importance of classifying and compartmentalizing sensitive communications, as many of the exfiltrated cables contained information that should have been transmitted through higher-classification systems unavailable to the attackers (Rid, 2020).

The Vienna Convention and Its Digital Gaps. The Vienna Convention on Diplomatic Relations (1961) remains the primary international legal instrument governing the protection of diplomatic communications. Article 27 of the Convention establishes that the receiving state shall permit and protect free communication on the part of the diplomatic mission for all official purposes. The Convention further provides that the official correspondence of the mission shall be inviolable and that the diplomatic bag shall not be opened or detained. These provisions were designed to protect physical communications from interception and interference by host state authorities (United Nations, 1961).

The application of these norms to digital communications is contested and unresolved. While some

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

scholars argue that the Convention's general principles extend to digital communications by analogy just as physical pouches are inviolable, so too should be encrypted digital channels others maintain that the Convention's specific provisions address only physical correspondence and that additional treaty obligations are required to extend equivalent protections to the cyber domain (Dinniss, 2012). The Tallinn Manual 2.0, a non-binding scholarly assessment of international law applicable to cyber operations, acknowledges the ambiguity surrounding diplomatic communications in cyberspace but stops short of resolving the fundamental question of whether cyber intrusions violate the Vienna Convention's inviolability provisions (Schmitt, 2017).

Emerging Cyber Norms and Their Limitations. Efforts to develop international norms governing state behavior in cyberspace have produced modest results. The United Nations Group of Governmental Experts (UN GGE) has reached consensus on a limited set of voluntary norms, including the principle that states should not knowingly allow their territory to be used for internationally wrongful cyber acts against other states and that critical infrastructure should be protected from cyber attacks during peacetime (UN GGE, 2015). The establishment of the Open-Ended Working Group (OEWG) in 2019 broadened participation in cyber norm development to include non-Western states previously excluded from GGE discussions (Schmitt & Vihul, 2017).

Despite these advances, the normative framework remains inadequate for several reasons. First, the norms developed through the GGE and OEWG process are voluntary and non-binding, lacking enforcement mechanisms. Second, attribution of cyberattacks to specific state actors remains technically challenging and diplomatically fraught, limiting the practical application of accountability norms. Third, major cyber powers including Russia and China have advocated for a fundamentally different normative architecture one emphasizing state sovereignty over information flows rather than individual rights and free expression creating deep structural divisions in international cyber governance (Mueller, 2017).

Technical Safeguards. Effective protection of diplomatic communications requires a comprehensive technical security architecture layered across endpoints, networks, and data. At the endpoint level, diplomatic devices must be configured with full-disk encryption, hardware security modules for credential storage, and endpoint detection and response (EDR) capabilities that enable rapid identification and containment of malicious activity. Multi-factor authentication using hardware security keys not SMS-based codes vulnerable to SIM-swapping should be mandatory for access to all sensitive systems (NIST, 2020). Foreign ministries should implement zero-trust network architectures that treat every user and device as potentially compromised and require continuous verification rather than relying on perimeter-based trust models.

Network-level controls should include robust segmentation between classified and unclassified systems, encrypted virtual private networks for all remote access, and deep packet inspection capabilities that can detect exfiltration attempts. End-to-end encrypted messaging applications built on open-source cryptographic standards such as Signal Protocol should replace commercial platforms for sensitive diplomatic communications. Several European governments have already deployed sovereign encrypted communications platforms, including France's Tchap system and Germany's IVBB network, which demonstrate the technical feasibility of this approach for mid-sized diplomatic services (Bonfante et al., 2019).

Supply chain security deserves particular attention given the lessons of the SolarWinds incident. Foreign ministries should maintain comprehensive software bills of materials (SBOM) for all systems, conduct rigorous vendor security assessments, and implement cryptographic verification of software updates before deployment. Where operationally feasible, preference should be given to open-source

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

software whose code can be independently audited over proprietary solutions from vendors whose security practices cannot be independently verified.

Institutional and Human Security Measures. Technical controls alone cannot secure diplomatic communications in the absence of complementary institutional and human security measures. Foreign ministries should establish dedicated cybersecurity functions within their organizational structures, staffed by professionals who combine technical expertise with understanding of diplomatic processes and security culture. Regular security awareness training—addressing phishing recognition, secure communications practices, and incident reporting should be mandatory for all diplomatic personnel, including senior officials who may be resistant to behavioral constraints on their communications practices (Cialdini, 2021).

Compartmentalization principles should govern access to sensitive communications. The principle of least privilege access only to information required for specific duties should be systematically applied, with regular access reviews to ensure that personnel who change roles or leave service do not retain access to sensitive systems. Insider threat detection programs combining behavioral analytics and counterintelligence awareness can help identify personnel who may be subject to foreign recruitment or who exhibit patterns of unusual data access (Gelles, 2016). These programs must be balanced against civil liberties and labor rights considerations, and their implementation should be governed by clear legal frameworks and oversight mechanisms.

The cybersecurity challenges facing diplomatic institutions in advanced economies are substantially amplified in developing countries, where foreign ministries often operate with severely constrained budgets, limited technical expertise, and reliance on commercial or foreign-provided communications infrastructure. Many African, Latin American, and Pacific island states lack the resources to deploy sophisticated endpoint detection systems, conduct regular security audits, or recruit and retain qualified cybersecurity professionals. These institutional gaps create opportunities for both powerful state actors and criminal organizations to compromise diplomatic communications with relative impunity (ITU, 2021).

International organizations, regional bodies, and technologically capable states have a responsibility to support cybersecurity capacity building among diplomatically underserved countries. The International Telecommunication Union's Global Cybersecurity Agenda and the UN's capacity-building mandate under the OEWG framework provide institutional vehicles for such assistance. Practical support might include training programs for diplomatic cybersecurity personnel, provision of open-source encryption tools and secure communications platforms, threat intelligence sharing arrangements, and assistance with developing national cyber incident response capabilities (ITU, 2021). The European Union's cyber capacity building programs, delivered through the EU Cyber Direct initiative, offer a model for structured multilateral engagement on diplomatic cybersecurity.

South-South cooperation in cybersecurity capacity building also holds significant promise. Regional groupings such as the African Union, ASEAN, and the Community of Latin American and Caribbean States have developed regional cybersecurity frameworks that can serve as vehicles for sharing expertise, coordinating incident response, and developing common technical standards for diplomatic communications systems. The establishment of regional Computer Emergency Response Teams (CERTs) with mandates extending to diplomatic infrastructure would significantly enhance the collective resilience of diplomatically underserved regions against targeted cyber operations.

Based on the foregoing analysis, this article advances the following policy recommendations for foreign ministries, international organizations, and cybersecurity practitioners.

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Foreign ministries should accelerate the transition to zero-trust network architectures and mandatory end-to-end encryption for all sensitive diplomatic communications. Investment in sovereign encrypted communications infrastructure, modeled on existing European examples, should be a priority for states with the technical and financial capacity to develop such systems. All diplomatic personnel should receive regular, mandatory cybersecurity training, with particular emphasis on social engineering and phishing recognition.

At the international level, states should work through the United Nations OEWG to develop legally binding instruments governing cyber operations against diplomatic infrastructure, building on but extending beyond the existing voluntary norm framework. The explicit extension of the Vienna Convention's inviolability protections to digital communications should be pursued through a formal interpretive process, potentially including an Additional Protocol to the Convention. Existing bilateral and multilateral diplomatic communications channels should be leveraged to establish direct hotlines and incident notification mechanisms for cyber incidents affecting diplomatic infrastructure.

The international community should significantly increase investment in cybersecurity capacity building for developing states, recognizing that the integrity of the global diplomatic system depends on the security of its weakest links. Technology transfer arrangements and open-source security solutions can help bridge the resource gap between advanced and developing diplomatic services. Regional CERTs with diplomatic cybersecurity mandates should be established and adequately funded across all world regions.

Conclusion

The protection of diplomatic communications in the digital age demands a fundamental rethinking of the legal, institutional, and technical frameworks that have traditionally governed diplomatic security. The digitalization of diplomacy has created enormous efficiencies and opened new channels of engagement, but it has simultaneously exposed the world's diplomatic networks to unprecedented threats from sophisticated state-sponsored actors, criminal organizations, and other adversaries. The case studies examined in this article from the SolarWinds supply chain compromise to the systematic exfiltration of EU diplomatic cables demonstrate that these threats are neither theoretical nor marginal, but present and consequential.

Effective response requires action on multiple fronts simultaneously. Technically, foreign ministries must embrace zero-trust architectures, end-to-end encryption, and supply chain security practices that reflect the realities of modern threat environments. Institutionally, diplomatic cultures must evolve to prioritize cybersecurity as a core competency rather than a peripheral IT concern, with dedicated professional expertise and comprehensive personnel security programs. Legally, the international community must close the normative gap between the Vienna Convention's paper-age inviolability protections and the requirements of digital diplomacy, developing binding instruments that impose genuine accountability for cyber intrusions against diplomatic infrastructure.

Perhaps most importantly, the protection of diplomatic communications must be understood as a collective challenge requiring collective solutions. The integrity of the international diplomatic system—the infrastructure through which states negotiate their differences, build cooperative arrangements, and prevent conflicts from escalating—depends on the confidentiality and reliability of the communications that sustain it. Investing in the security of that infrastructure is not merely a technical necessity but a strategic imperative for all states committed to the maintenance of international order in the digital age.

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

References

1. Area 1 Security. (2018). Phishing diplomacy: Hacking EU foreign policy. Area 1 Security White Paper.
2. Bjola, C., & Holmes, M. (Eds.). (2015). Digital diplomacy: Theory and practice. Routledge.
3. Bjola, C., & Zeng, J. (2017). Diplomatic signalling in the age of social media. Cambridge Review of International Affairs, 30(1), 55–75. https://doi.org/10.1080/09557571.2016.1264649
4. Bonfante, G., Kaczmarek, M., & Zemmouri, S. (2019). Sovereign cloud and encrypted communications for European governments. Journal of Cybersecurity and Privacy, 1(2), 12–29.
5. Cialdini, R. B. (2021). Influence: The psychology of persuasion (New and expanded ed.). Harper Business.
6. Cybersecurity and Infrastructure Security Agency. (2021). Alert (AA21-008A): Detecting post-compromise threat activity in Microsoft cloud environments. U.S. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/alerts/aa21-008a
7. Dinniss, H. H. (2012). Cyber warfare and the laws of war. Cambridge University Press.
8. FireEye. (2020). APT41: A dual espionage and cyber crime operation. FireEye Threat Intelligence Report. Mandiant.
9. Gelles, M. G. (2016). Insider threat: Prevention, detection, mitigation, and deterrence. Butterworth-Heinemann.
10. Hocking, B., & Melissen, J. (2015). Diplomacy in the digital age. Netherlands Institute of International Relations 'Clingendael'.
11. International Telecommunication Union. (2021). Global Cybersecurity Index 2020. ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
12. Kosseff, J. (2018). Defining cybersecurity law. Iowa Law Review, 103(3), 985–1031.
13. Mandiant. (2021). Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor. Mandiant Threat Research Blog.
14. Microsoft. (2021). A moment of reckoning: The need for a strong and global cybersecurity norm. Microsoft On the Issues Blog. https://blogs.microsoft.com/on-the-issues/2021/02/14/moment-reckoning-cybersecurity/
15. Mueller, M. L. (2017). Will the Internet fragment? Sovereignty, globalization and cyberspace. Polity Press.
16. National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207
17. Oltsik, J. (2019). The life and times of cybersecurity professionals. Enterprise Strategy Group and Information Systems Security Association.
18. Rid, T. (2013). Cyber war will not take place. Oxford University Press.
19. Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
20. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
21. Sanger, D. E. (2018). The perfect weapon: War, sabotage, and fear in the cyber age. Crown Publishers.
22. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
23. Schmitt, M. N., & Vihul, L. (2017). International cyber law politicized: The UN GGE's failure to advance cyber norms. Just Security. https://www.justsecurity.org/42768/international-cyber-law-politicized/
24. Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.
25. United Nations. (1961). Vienna Convention on Diplomatic Relations. United Nations Treaty Series, 500, 95.
26. United Nations Group of Governmental Experts. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of

Volume: 5 Issue: 04 | Apr–2026 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

international security (A/70/174). United Nations General Assembly.
27. Verizon. (2022). 2022 Data breach investigations report. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/