Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 10, 2025

TOWARD A NEW CYBER WORLD ORDER: CYBER DIPLOMACY AND THE CHANGING NATURE OF INTERNATIONAL RELATIONS

Muhammad Bilal Shakeel[1], Urooj Bashir[2], Muhammad Sameer Imran[*3], Muhammad Junaid Abbas[4]

[1] *Department of Political Science and International Relations, University of Sargodha.*
[2] *Assistant Professor, M.A. Raoof College of Law, The University of Lahore.*
[*3] *Department of School of Journalism and Communication, University of Shanghai University.*
[4] *Department of Computer and Information Sciences, University of Strathclyde.*

[*3]muhammadsameerimran12@gmail.com

DOI: https://doi.org/10.5281/zenodo.17482322

Keywords:
Cyberspace, Cyber Diplomacy, Cyber World Order, Cybercrime, Open-Ended Working Group

Article History
Received: 10 September 2025
Accepted: 16 October 2025
Published: 30 October 2025

Corresponding Author: *
Muhammad Sameer Imran

Abstract

Cyber diplomacy is redefining international relations by shaping a "Cyber World Order" grounded in evolving norms, technological interdependence, and multilateral engagement. This paper examines its role in global cyber governance, focusing on the UN Open-Ended Working Group (OEWG) on ICT security, whose 2025 Final Report established a permanent UN mechanism and Dedicated Thematic Groups on state behaviour and capacity building. Against a backdrop of a 72% rise in perceived cyber risks and escalating geopolitical tensions spanning U.S.-China cyber operations, Russia-Ukraine conflicts, and global surveillance concerns states pursue divergent governance models: U.S. digital policy and AI integration, China's data sovereignty, Russia's information security norms, and the EU's regulatory harmonization under NIS2. The forthcoming UN Convention Against Cybercrime (2025) and regional frameworks like NATO's cybersecurity strategies and ASEAN initiatives reflect growing cooperation yet expose enforcement and trust challenges. With global cybercrime costs projected at $10.5 trillion, the study underscores cyber diplomacy's potential to balance security, sovereignty, and collaboration. It advocates for an inclusive "Cyber Diplomacy 2.0" that strengthens multilateralism, technology governance, and equitable capacity building to ensure a stable and cooperative digital order.

1. INTRODUCTION

1.1 Defining Cyber Diplomacy: From Statecraft to Digital Governance

Cyber diplomacy, an evolving facet of international statecraft, refers to the strategic use of diplomatic tools to address issues in cyberspace, encompassing negotiations, norm-setting, and cooperation to manage digital interactions among states, non-state actors, and international organizations. Unlike traditional diplomacy, it operates in a domain unbound by physical borders, where state behavior, cybersecurity, and data governance intersect. Recent frameworks, such as the UN Open-Ended Working Group (OEWG) on ICT security (2021-2025), highlight its shift from ad hoc responses to structured multilateral engagement, with the July 2025 Final

Report establishing a permanent UN mechanism to foster dialogue and accountability. Cyber diplomacy now integrates emerging technologies like AI, addressing threats like the 42% rise in phishing attacks reported in 2024, while navigating divergent national priorities, from data sovereignty to open internet advocacy. (Affairs, 2025)

Cyberspace has emerged as the fifth domain of international relations, alongside land, sea, air, and space, fundamentally altering state interactions, power dynamics, and global governance. It serves as a platform for cooperation, competition, and conflict, with incidents like the 70% surge in state-linked cyber operations in the Russia-Ukraine context in 2024 and mutual attributions of espionage among major powers illustrating its geopolitical weight. Global cybercrime costs, projected at $10.5 trillion for 2025, (Ventures, 2020) underscore economic stakes, while initiatives like regional digital strategies highlight their role in reshaping alliances and influence. Cyberspace challenges traditional notions of sovereignty, demanding new diplomatic approaches to address hybrid threats and cross-border data flows.

Table 1: Comparative Overview of Major Powers' Cyber Diplomacy Strategies

Country	Core Strategy	Key Policy Documents	Focus Areas	Diplomatic Outlook
United States	Multilateral cooperation, AI integration	Bureau of Cyberspace and Digital Policy (2022), AI Action Plan (2025)	Open internet, AI-driven security, NATO alignment	Advocates open digital order and collective defense
China	Data sovereignty and state control	Data Security Law (2021), Global Data Security Initiative	Data localization, state-led governance	Promotes sovereign internet and digital independence
Russia	Information security and cyber sovereignty	UN cyber norms proposals (2024)	National network control, state-centric regulation	Supports strict sovereignty and limited global governance
European Union	Regulatory harmonization	NIS2 Directive (2024)	Risk management, privacy, multilateral cooperation	Balances sovereignty with open, rules-based cyberspace

This paper argues that cyber diplomacy is a pivotal force in forging a new Cyber World Order, characterized by evolving norms, contested governance models, and redefined international relations. By facilitating agreements like the UN Convention against Cybercrime, set for signatures on October 25, 2025, in Hanoi, and fostering norms of responsible state behavior, cyber diplomacy seeks to balance cooperation with competition. However, divergent approaches—ranging from multilateral frameworks to unilateral policies—highlight tensions that could lead to either a cohesive global order or a fragmented digital landscape, reshaping power, trust, and stability in international relations.

The study focuses on the period 2021-2025, analyzing key developments such as the OEWG's outcomes, the UN Convention's framework, and regional strategies like the EU's NIS2 Directive. It employs a mixed methodology, combining qualitative analysis of policy documents, UN reports, and academic literature with case studies of significant cyber incidents (e.g., geopolitical cyberattacks in 2024). Statistical data from sources like the World Economic Forum's Cybersecurity Outlook 2025 and industry reports provide quantitative insights into trends like the 72% rise in perceived cyber risks. The analysis remains unbiased, examining diverse perspectives from global powers, regional blocs, and non-state actors

to assess cyber diplomacy's impact on international relations. (Forum, 2025)

2. The Genesis of Cyber Diplomacy in Global Governance

2.1 Early Cyber Diplomacy: From Bilateral Talks to Multilateral Efforts (2000s-2010s)

Cyber diplomacy emerged in the early 2000s as states grappled with the growing significance of cyberspace in global interactions. Initial efforts were largely bilateral, driven by incidents like the 2007 cyberattacks on Estonia, attributed to state-linked actors, ((CCDCOE), 2008) which prompted dialogues between NATO members and other nations on cybersecurity cooperation. The Budapest Convention on Cybercrime (2001), the first international treaty of its kind, marked a pivotal shift toward multilateral frameworks, focusing on harmonizing laws and fostering cross-border investigations, though its adoption was limited to 68 countries by 2010 due to concerns over sovereignty and enforcement. During this period, major powers like the U.S. and China engaged in early cyber dialogues, such as the 2009 U.S.-China cybersecurity talks, which aimed to address espionage concerns but often stalled due to mistrust and differing governance models. These efforts laid the groundwork for cyber diplomacy, highlighting the need for broader, inclusive frameworks to address the transnational nature of cyber threats. (Europe, 2001)

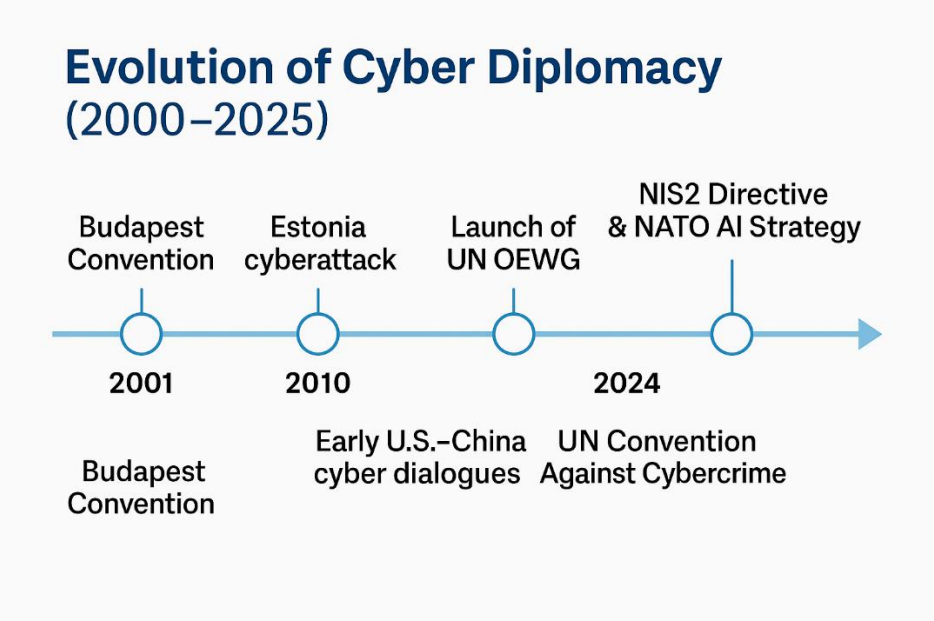

Figure 2: Evolution of Cyber Diplomacy (2000–2025)

2.2 UN-Led Initiatives: OEWG (2021-2025) and the Global Mechanism's Role

The United Nations has played a central role in advancing cyber diplomacy through structured multilateral platforms. The Open-Ended Working Group (OEWG) on ICT security (2021-2025), established under UN General Assembly Resolution 75/240, facilitated global discussions on responsible state behavior, culminating in its July 2025 Final Report. This report endorsed a permanent UN mechanism and two Dedicated Thematic Groups (DTGs) to focus on norm implementation, capacity building, and threat mitigation, involving 193 member states and non-state stakeholders. The Global Mechanism, a key outcome, aims to operationalize cyber norms, such as protecting critical infrastructure, as evidenced by the 2023 UN consensus on applying international law to cyberspace.

These initiatives reflect a maturing diplomatic approach, bridging diverse perspectives from the Global South, ASEAN, and major powers, though

challenges remain in reconciling differing priorities, such as data sovereignty versus open internet principles. (Assembly, 2020)

2.3 Shift to a Cyber World Order: Norms, Accountability, and Power Redistribution

Cyber diplomacy is driving the emergence of a Cyber World Order, characterized by evolving norms, accountability mechanisms, and a redistribution of global power. Norms like transparency in cyber operations and attribution of attacks, endorsed by the OEWG, aim to foster trust, yet their non-binding nature limits enforcement, as seen in the 2024 surge of unattributed incidents (e.g., 1,636 weekly attacks per organization globally). Accountability efforts, such as the UN Convention against Cybercrime (set for signatures on October 25, 2025, in Hanoi), seek to standardize responses to cybercrime, projected to cost $10.5 trillion globally in 2025, but face hurdles over jurisdictional disputes. Power redistribution is evident in initiatives like regional digital frameworks, which empower smaller states and non-state actors, including tech firms, to influence norm-setting, challenging traditional state-centric IR models. This shift underscores cyber diplomacy's role in redefining global governance, balancing cooperation with competitive dynamics in an interconnected digital era. (Research, 2024)

3. State and Non-State Actors in Shaping Cyber Diplomacy

3.1 Major Powers' Strategies: US Cyber Diplomacy Bureau, China's Data Security Law, Russia's Cyber Sovereignty

Major powers play a pivotal role in shaping cyber diplomacy through distinct national strategies that reflect their geopolitical priorities. The United States, through its Bureau of Cyberspace and Digital Policy, established in 2022 and enhanced by the 2025 AI Action Plan, emphasizes multilateral cooperation and AI integration to counter threats, as seen in its leadership in NATO's cybersecurity frameworks and advocacy for open internet principles. China's Data Security Law (2021) and Global Data Security Initiative prioritize data sovereignty and state control, shaping its diplomatic engagements, particularly in forums like the Shanghai Cooperation Organization, to counterbalance Western influence. Russia advocates for cyber sovereignty, emphasizing national control over information flows, as evidenced by its 2024 proposals at the UN for stricter cyber norms and its push for the UN Convention against Cybercrime, set for signatures in October 2025. These strategies, while divergent, collectively drive global cyber diplomacy by framing debates on governance, security, and norms, often creating tensions between open and controlled internet models. (State, 2022)

3.2 Non-State Influence: Tech Giants (e.g., Microsoft's Cyber Norms Advocacy) and Hacktivist Groups

Non-state actors, particularly tech giants and hacktivist groups, significantly influence cyber diplomacy by shaping norms and amplifying cyber incidents. Companies like Microsoft, through initiatives like the 2023 Digital Peace Campaign, advocate for global cyber norms, such as protecting civilian infrastructure, and collaborate with governments on attribution and threat intelligence, as seen in their reports on 2024 cyberattacks linked to geopolitical conflicts. Other tech firms, including Google and Amazon, contribute to cybersecurity standards, influencing policies like the EU's NIS2 Directive. Hacktivist groups, such as Anonymous, disrupt state and corporate systems, with a 30% rise in hacktivist-driven incidents in 2024, complicating diplomatic efforts by introducing unpredictable actors. These non-state entities challenge state-centric diplomacy, necessitating inclusive frameworks that integrate private sector expertise and address decentralized threats. (Corporation, 2020)

3.3 Multilateral Platforms: UN, NATO, and ASEAN's Role in Cyber Norm Consensus

Multilateral platforms are central to forging consensus on cyber norms, bridging state and non-state perspectives. The United Nations, through the Open-Ended Working Group

(OEWG) on ICT security (2021-2025), has facilitated global dialogue, culminating in the July 2025 Final Report that established a permanent mechanism and Dedicated Thematic Groups to advance norms like transparency and capacity building. NATO's 2025 Cybersecurity Strategy emphasizes collective defense, integrating AI and quantum resilience to address threats like the 1,636 weekly cyberattacks per organization reported in 2024. ASEAN's Cybersecurity Cooperation Strategy (2023-2025) focuses on regional resilience, fostering norms like cross-border data sharing, critical for addressing the 42% rise in phishing attacks in the region. These platforms, despite challenges like geopolitical divergences, drive the Cyber World Order by promoting inclusive norm-setting and cooperation, balancing diverse interests in a contested digital landscape. ((C2COE), 2025)

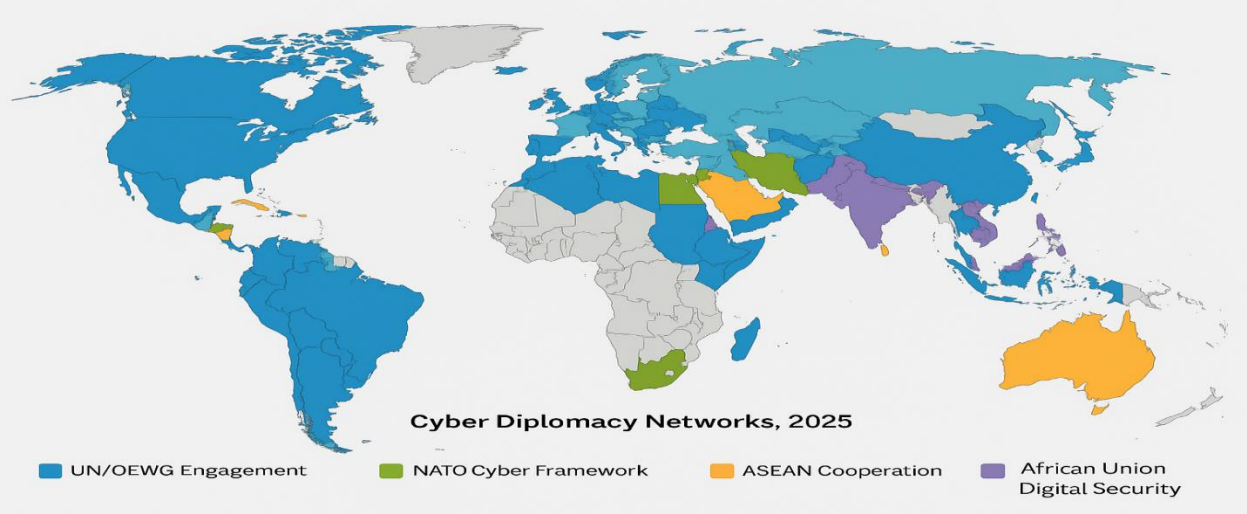

Figure 1: Global Map of Cyber Diplomacy Networks (2025)

Geopolitical Cyber Conflicts and Their Diplomatic Fallout

3.4 2024-2025 Trends: 70% Surge in State-Sponsored Attacks (e.g., Russia-Ukraine Cyber Operations)

The period 2024-2025 has witnessed a significant escalation in state-sponsored cyberattacks, with a reported 70% surge in such incidents globally, driven by geopolitical tensions and strategic rivalries. The Russia-Ukraine conflict exemplifies this trend, with 4,315 documented cyber operations in 2024, targeting critical infrastructure like energy grids and communication networks, aimed at disrupting military and civilian operations. Beyond this, global reports indicate a 72% rise in perceived cyber risks, with 1,636 weekly attacks per organization, reflecting a broader trend of state actors leveraging cyberspace for strategic advantage. These attacks, often involving sophisticated malware and social engineering (e.g., a 42% increase in phishing incidents), underscore the growing integration of cyber operations into geopolitical strategies, complicating diplomatic efforts to maintain stability and cooperation. (Microsoft, 2024)

3.5 Case Studies: US-China Cyber Espionage, Iran's Ransomware Campaigns

Two prominent case studies highlight the diversity and impact of geopolitical cyber conflicts. US-China cyber espionage has intensified, with mutual attributions of data breaches and intellectual property theft. In 2024, the U.S.

identified advanced persistent threats (APTs) linked to Chinese actors targeting critical sectors, while China accused U.S. entities of infiltrating its networks, straining bilateral dialogues despite efforts like the 2023 US-China cybersecurity working group. Separately, Iran's ransomware campaigns, targeting regional adversaries and global entities, surged in 2024, with groups like Pay2Key deploying ransomware against infrastructure, demanding payments while advancing geopolitical objectives. These incidents, often unclaimed or ambiguously attributed, challenge diplomatic attribution mechanisms and erode trust, as states struggle to align responses within frameworks like the UN's OEWG or the upcoming UN Convention against Cybercrime (October 2025). (Mandiant, 2024)

3.6 Impact on International Relations: Trust Deficits and Hybrid Conflict Escalation

Geopolitical cyber conflicts significantly reshape international relations by fostering trust deficits and escalating hybrid warfare. The surge in unattributed or contested cyberattacks, coupled with a projected $10.5 trillion in global cybercrime costs for 2025, undermines confidence in interstate cooperation, as seen in stalled US-China talks and regional tensions following Iran's campaigns. Hybrid conflicts, blending cyber and physical operations, have intensified, with NATO reporting a 30% increase in hybrid threats in 2024, prompting alliances to bolster collective defense strategies like the 2025 Cybersecurity Strategy. These dynamics challenge traditional notions of sovereignty, as states navigate blurred lines between cyber aggression and legitimate defense, necessitating diplomatic innovations like the UN's Dedicated Thematic Groups to restore trust and mitigate escalation risks. The resulting fragmentation in global cyber governance underscores the urgency of cohesive diplomatic efforts to address these evolving threats. ((NATO), n.d.)

4. Building a Cyber World Order: International Agreements and Norms

4.1 The UN Convention Against Cybercrime (2025): Scope and Challenges

The UN Convention Against Cybercrime, set to open for signatures on October 25, 2025, in Hanoi, represents a landmark effort to establish a global framework for combating cybercrime, building on the UN Ad Hoc Committee's work from 2022-2025. Its scope includes harmonizing legal frameworks for cyber-dependent crimes, enhancing cross-border law enforcement cooperation, and addressing the $10.5 trillion global cybercrime cost projected for 2025. The convention emphasizes victim protection and technical assistance, particularly for developing nations, but faces challenges such as divergent state priorities—some advocate for robust enforcement, while others raise concerns over potential surveillance overreach and vague definitions of cybercrime. Implementation hurdles, including varying judicial capacities and geopolitical tensions, threaten its effectiveness, necessitating diplomatic efforts to ensure broad adoption and compliance. (Crime, n.d.)

4.2 Regional Frameworks: EU's NIS2 Directive, African Union's Cybersecurity Strategy

Regional frameworks complement global efforts by addressing localized cyber threats and governance needs. The EU's Network and Information Security Directive 2 (NIS2), implemented in 2024, strengthens cybersecurity across member states by mandating risk management, incident reporting, and cross- sector cooperation, covering critical sectors like energy and healthcare. It responds to the 42% rise in phishing attacks in 2024, aiming to enhance resilience through harmonized standards. The African Union's Cybersecurity Strategy (2020-2025), extended in 2024, focuses on capacity building, legal frameworks, and regional cooperation to address Africa's 15% share of global cyberattacks, emphasizing the Malabo Convention's enforcement. While both frameworks foster regional cohesion, they face challenges like resource disparities and alignment

with global norms, highlighting the need for interoperable standards to support a unified Cyber World Order. (Commission, 2023)

Table 2: Key Global and Regional Cybersecurity Frameworks (2021–2025)

Framework	Year	Scope	Objectives	Challenges
UN OEWG on ICT Security	2021–2025	Global	Establish cyber norms, promote transparency, build capacity	Non-binding norms, lack of enforcement
UN Convention Against Cybercrime	2025	Global	Harmonize cybercrime laws, cross-border cooperation	Jurisdictional disputes, enforcement gaps
EU NIS2 Directive	2024	Regional (Europe)	Strengthen network resilience, harmonize security standards	Implementation differences across member states
ASEAN Cybersecurity Cooperation Strategy	2023–2025	Regional (Asia)	Capacity building, cross-border data flow regulation	Resource disparity, regional coordination
African Union Cybersecurity Strategy	2020–2025	Regional (Africa)	Capacity building, harmonized legal frameworks	Limited funding, technical expertise gaps

4.3 Gaps in Global Consensus: Divergent Views on Cyber Sovereignty vs. Open Internet

Global consensus on cyber norms remains elusive due to competing visions of cyberspace governance. Advocates of cyber sovereignty, such as China and Russia, prioritize state control over digital infrastructure and data flows, as seen in China's Data Security Law and Russia's 2024 UN proposals for stricter information security norms. In contrast, proponents of an open internet, including the U.S. and EU, emphasize free data flows and global connectivity, as reflected in the U.S. International Cyberspace & Digital Policy. These divergences, evident in debates during the UN OEWG (2021-2025), hinder agreement on issues like data localization and surveillance, with 193 member states struggling to reconcile priorities. Such gaps risk fragmenting the Cyber World Order, underscoring the need for inclusive diplomatic dialogues.

4.4 Emerging Norms: Accountability, Attribution, and Responsible State Behavior

Emerging cyber norms aim to foster stability and accountability in cyberspace. The UN OEWG's 2025 Final Report endorses norms like responsible state behavior, transparency in cyber operations, and protection of critical infrastructure, building on the 2023 UN consensus on applying international law to cyberspace. Attribution mechanisms, supported by initiatives like Microsoft's threat intelligence sharing, enhance accountability by identifying state and non-state actors behind incidents like the 1,636 weekly cyberattacks per organization in 2024. However, non-binding norms and varying attribution standards, coupled with geopolitical rivalries, limit enforcement, as seen in contested attributions in 2024 cyber incidents. These norms, while foundational to a cohesive Cyber World Order, require stronger diplomatic commitments to ensure consistent application and global trust.

5. Emerging Technologies and Their Role in Cyber Diplomacy

5.1 AI in Cyber Diplomacy: AI-Powered Attacks and Defensive Pacts (e.g., NATO's AI Strategy)

Artificial Intelligence (AI) is reshaping cyber diplomacy by amplifying both offensive and

defensive capabilities in cyberspace. AI-powered attacks, leveraging machine learning for sophisticated malware and automated phishing, contributed to a 97 billion exploitation attempts globally in 2024, necessitating diplomatic responses to regulate such technologies. NATO's 2025 AI Strategy, adopted to enhance collective defense, integrates AI for threat detection and response, fostering pacts among member states to counter AI-driven threats while promoting ethical use. Concurrently, the UN's Open-Ended Working Group (OEWG) 2025 Final Report highlights AI governance as a priority, with Dedicated Thematic Groups exploring norms to mitigate AI misuse in cyberattacks. These efforts reflect AI's dual role as a diplomatic challenge and opportunity, requiring global cooperation to balance innovation with security. (Summary of NATO's revised Artificial Intelligence (AI) strategy, 2024)

5.2 Quantum Computing: Implications for Encryption and Diplomatic Negotiations

Quantum computing poses transformative implications for cyber diplomacy, particularly in undermining current encryption standards. With quantum advancements potentially decrypting widely used algorithms by the 2030s, states are prioritizing post-quantum cryptography, as seen in the U.S. National Institute of Standards and Technology's 2024 quantum-resistant standards release. Diplomatically, quantum risks drive negotiations, with forums like the UN OEWG advocating for cooperative research and standards to secure global communication networks. Regional blocs, such as the EU's Quantum Flagship program, integrate quantum resilience into cybersecurity strategies, shaping diplomatic agendas to address future vulnerabilities. These negotiations underscore the need for proactive diplomacy to mitigate quantum threats and maintain trust in digital infrastructures. (NIST Releases First 3 Finalized Post-Quantum Encryption Standards, 2024)

5.3 Cybercrime Trends: 42% Rise in Phishing, Social Engineering in 2024

Cybercrime trends, particularly a 42% increase in phishing and social engineering attacks in 2024, highlight the evolving threat landscape influencing cyber diplomacy. These human-centric attacks, often exploiting trust in digital systems, contributed to the projected $10.5 trillion global cybercrime cost in 2025, disproportionately affecting under-resourced regions. The UN Convention Against Cybercrime (set for signatures in October 2025) addresses these trends by promoting international cooperation on prevention and victim support, yet faces challenges in standardizing responses across diverse legal systems. Diplomatic efforts, including ASEAN's Cybersecurity Cooperation Strategy, prioritize capacity building to counter social engineering, reflecting the need for global and regional strategies to tackle these pervasive threats.

5.4 Technology as a Diplomatic Lever: Data Governance and Cross-Border Data Flows

Emerging technologies serve as diplomatic levers in shaping data governance and cross-border data flows, critical to the Cyber World Order. Divergent approaches—such as China's Data Security Law emphasizing state control and the EU's General Data Protection Regulation (GDPR) prioritizing user rights—fuel diplomatic tensions over data sovereignty versus global connectivity. Initiatives like the African Union's Cybersecurity Strategy advocate for regional data frameworks to address the 15% share of global cyberattacks, fostering cooperation on data flows. The UN OEWG's 2025 outcomes emphasize norms for transparent data governance, yet geopolitical rivalries hinder consensus, as seen in debates over the UN Convention's data-sharing provisions. Technology-driven diplomacy thus requires inclusive frameworks to harmonize data policies and ensure equitable access in a digitally interconnected world. (Naida Dzigal, 2025)

6. Transforming International Relations: A New Cyber World Order

6.1 Redefining Sovereignty: Cyberspace as a Contested Domain

Cyberspace has redefined sovereignty in international relations (IR), emerging as a contested domain where traditional state authority is challenged by borderless digital interactions. Unlike physical territories, cyberspace enables states, non-state actors, and individuals to exert influence beyond national boundaries, complicating notions of control and jurisdiction. The UN Open-Ended Working Group (OEWG) 2025 Final Report underscores the need for norms respecting digital sovereignty, yet disagreements persist, with some states advocating for absolute control over national networks and others supporting a shared global cyberspace. Incidents like the 2024 surge in cyberattacks (1,636 weekly attacks per organization) highlight how states navigate sovereignty disputes, using cyber operations to assert influence while facing challenges in attributing and regulating cross-border actions. This redefinition necessitates diplomatic frameworks to balance national autonomy with global cooperation, shaping a Cyber World Order where sovereignty is fluid and contested.

6.2 Power Shifts: Cyber Capabilities and Global Influence (e.g., China's Digital Silk Road)

Cyber capabilities are driving power shifts in IR, with states leveraging technological prowess to enhance global influence. China's Digital Silk Road, an extension of the Belt and Road Initiative, has expanded digital infrastructure across 60 countries by 2025, strengthening economic and diplomatic ties through 5G networks and data centers, thereby amplifying China's role in global cyber governance. Similarly, the U.S. harnesses its advanced cyber capabilities through the Bureau of Cyberspace and Digital Policy, shaping norms via multilateral forums like the UN and NATO. Developing nations, supported by initiatives like the African Union's Cybersecurity Strategy, are also gaining influence by adopting cyber frameworks, though resource disparities limit their impact. These shifts, driven by technological advancements and strategic investments, redefine global power dynamics, positioning cyber diplomacy as a key instrument in the emerging Cyber World Order. (Mochinaga, 2025)

6.3 Alliances and Rivalries: Cyber Pacts (e.g., AUKUS Cyber Framework) vs. Authoritarian Blocs

The Cyber World Order is shaped by competing alliances and rivalries, with cyber pacts and blocs redefining IR. The AUKUS Cyber Framework, expanded in 2024, enhances cybersecurity cooperation among Australia, the UK, and the U.S., focusing on AI and quantum resilience to counter threats like the 70% surge in state-sponsored attacks in 2024. In contrast, authoritarian blocs, such as the Shanghai Cooperation Organization, led by China and Russia, promote cyber sovereignty and coordinated defense strategies, as seen in their 2024 UN proposals for stricter information security norms. These rival frameworks, alongside NATO's 2025 Cybersecurity Strategy and ASEAN's regional efforts, highlight a polarized landscape where alliances drive norm-setting but also exacerbate tensions, challenging diplomatic efforts to foster global consensus. (Andrade, 2025)

6.4 Economic Impacts: $10.5T Cybercrime Costs and Global Economic Stability

The economic ramifications of cyber activities profoundly impact IR, with global cybercrime costs projected to reach $10.5 trillion in 2025, equivalent to roughly 10% of global GDP. This financial burden, driven by incidents like the 42% rise in phishing and ransomware attacks in 2024, exacerbates economic disparities, particularly affecting developing nations with limited cybersecurity infrastructure. The UN Convention Against Cybercrime, set for signatures in October 2025, aims to mitigate these costs through international cooperation, but enforcement gaps persist. Cybercrime's economic toll influences diplomatic priorities, prompting states to integrate cybersecurity into trade agreements and development aid, as seen in the EU's NIS2

Directive and regional frameworks. These economic pressures underscore the need for a cohesive Cyber World Order to ensure global stability through robust diplomatic and economic strategies. (Department, 2024)

8. Conclusion

Cyber diplomacy has become a vital tool for managing global cybersecurity challenges and shaping a new Cyber World Order defined by evolving norms, technologies, and power dynamics. The UN Open-Ended Working Group (2021–2025) and upcoming initiatives like the UN Convention Against Cybercrime (October 2025) highlight growing international cooperation on responsible state behavior and capacity building. Regional efforts such as the EU's NIS2 Directive, NATO's Cybersecurity Strategy, and ASEAN's cyber frameworks strengthen collective defense amid rising state-sponsored attacks and escalating cybercrime costs. Yet, competing visions of cyber governance, particularly between advocates of cyber sovereignty and an open internet, risk fragmentation. The future stability of cyberspace depends on whether cyber diplomacy can reconcile these divides through inclusive, multilateral engagement—integrating the Global South, regulating emerging technologies like AI and quantum computing, and fostering trust in an increasingly contested digital domain.

References

1. (C2COE), N. C. (2025). *ESET – Cyber Defense Summit 2025: From Cyberspace to Cyber Battlefield*. Retrieved from NATO C2COE: https://c2coe.org/eset-cyber-defense-summit-2025-from-cyberspace-to-cyber-battlefield/
2. (CCDCOE), N. C. (2008). *Cyber attacks against Estonia 2007 – Case study*. Retrieved from NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
3. (NATO), N. A. (n.d.). *NATO's approach to counter information threats – Public summary*. Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_231905.htm?utm_source=chatgpt.com
4. Affairs, U. N. (2025). *Open-Ended Working Group on security of and in the use of information and communication technologies (2021–2025)*. New York: United Nations. Retrieved from https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf
5. Andrade, T. G. (2025). Cybersecurity in the digital era: Geopolitical impacts and structural challenges. *IOSR Journal of Humanities and Social Science, 30*, 30-44. doi:10.9790/0837-3001063044
6. Assembly, U. N. (2020). *A/RES/75/240 – Developments in the field of information and telecommunications in the context of international security*. New York: United Nations. Retrieved from https://docs.un.org/en/A/RES/75/240
7. Commission, E. (2023). *NIS2 Directive: securing network and information systems*. Retrieved from European Commission: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
8. Corporation, M. (2020). *Digital Peace in Cyberspace: An Invisible Pillar for the UN Sustainable Development Goals*. Retrieved from Microsoft Corporation: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Digital-Peace-Cyberspace-Invisible-Pillar-for-UN-Sustainable-Goals.pdf
9. Crime, U. N. (n.d.). *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*. Retrieved from UNODC Cybercrime Programme: https://www.unodc.org/unodc/cybercrime/ad_hoc_committee/home

10. Department, I. M. (2024). *Chapter 3 Cyber Risk: A Growing Concern for Macrofinancial Stability*. IMF. Retrieved from https://www.elibrary.imf.org/display/book/9798400257704/CH003.xml
11. Europe, C. o. (2001). *Convention on Cybercrime (Budapest Convention)*. Retrieved from Council of Europe Treaty Series No. 185: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
12. Forum, W. E. (2025). *Global cybersecurity outlook 2025*. Geneva: World Economic Forum. Retrieved from https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
13. Mandiant. (2024). *Mandiant Annual Threat Intelligence Report 2024*. Google Cloud Security. Retrieved from https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024
14. Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Redmond, WA: Microsoft Corporation. Retrieved from https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf
15. Mochinaga, D. (2025). The Digital Silk Road and China's Technology Influence in Southeast Asia. Retrieved from https://www.cfr.org/sites/default/files/pdf/mochinaga_the-digital-silk-road-and-chinas-technology-influence-in-southeast-asia_june-2021.pdf
16. Naida Dzigal, D. S. (2025). Digital Sovereignty and Geopolitics in the Field of DataProtection: A Comparison of the EU, China, and the USA. doi:10.13140/RG.2.2.29957.87522
17. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. (2024). Retrieved from NIST: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
18. Research, C. P. (2024). *22nd July – Threat Intelligence Report (Global cyber-attack trends Q2 2024)*. Retrieved from Check Point Research: https://research.checkpoint.com/2024/22nd-july-threat-intelligence-report/
19. State, U. D. (2022). *Bureau of Cyberspace and Digital Policy – Overview*. Retrieved from US Department of State: https://www.state.gov/bureau-of-cyberspace-and-digital-policy/
20. *Summary of NATO's revised Artificial Intelligence (AI) strategy*. (2024). Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_227237.htm#:~:text=NATO's%202021%20AI%20Strategy%20set,Reliability%2C%20Governability%20and%20Bias%20Mitigation.
21. Ventures, C. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Retrieved from U.S. Securities and Exchange Commission (SEC) Archives: https://www.sec.gov/Archives/edgar/data/736012/000168316820004004/intrusion_ex9901.htm?utm_source=chatgpt.com