Tech Diplomacy: A Comprehensive Framework for Addressing Critical Technologies

Kamel Dine Remili, Adel Belouchrani, Riad Hartani and Nadjoua Bouzourine

Abstract−This paper discusses the problem of addressing critical technologies through tech diplomacy. The latter has recently emerged as a strategic response to manage the geopolitical consequences that are induced by rivalry over the control of critical technologies. Despite the growing importance of these technologies in global politics, the relationship between technological competition and diplomatic governance remains insufficiently conceptualized. The existing research often lacks an integrated framework connecting critical technologies to geopolitical competition, diplomatic mechanisms, and global governance. Moreover, most analyses focus on state competition while the influence of private technology multinationals remains underexplored despite their major global role. To address this gap, we propose a comprehensive Tech Diplomacy Framework (TDF) which addresses the diplomatic dynamics in international relations that these technologies generate. The framework is subsequently applied to Low Earth Orbit satellite internet as an illustrative critical technology to validate the proposed framework and its applicability to the whole range of critical technologies.

***Keywords*−tech diplomacy, critical technology, tech diplomacy framework, private tech firms, satellite internet.**

I. Introduction

Technology has long been an important source of power, and a country's technological capabilities are widely understood to influence its economic competitiveness, political influence, and military strength. Historically, technological development was in many cases closely associated with the state. Major technological advances, including nuclear energy, aerospace systems, telecommunications, navigation technologies, and early computing, were often directly developed or substantially supported through public funding. These technologies supported a range of objectives including territorial governance, defence capabilities, administrative capacity, and economic development. While private firms also contributed, the state generally played a central role in setting technological priorities and providing strategic direction. Over time, particularly toward the end of the 20th century, globalization and the emergence of the internet contributed to a gradual transformation of the innovation system in many countries. Governments increasingly shifted away from direct technology development and moved toward supporting market-driven innovation and public–private partnerships [1], [2].

In the 21st century, technologies such as artificial intelligence (AI), semiconductors, cloud and quantum computing, biotechnology, nanotechnology, satellite communications, and robotics are reshaping every domain of human life and affecting economic structures, geopolitical dynamics, and social systems.

Manuscript received April 5, 2026; accepted June 2, 2026.

K. D. Remili and A. Belouchrani are with Electronics Department, EcoleNationalePolytechnique, Algiers, ALGERIA (e-mail: kamel_dine.remili@g.enp.edu.dz, adel.belouchrani@g.enp.edu.dz).

R. Hartaniis with Xona Partners, USA (e-mail: riad@xonapartners.com).

N. Bouzourine is with Department of Public Policies and Comparative Systems, Ecole Nationale Supérieure De Sciences Politiques (e-mail: bouzourine.nadjoua@enssp.dz).

Digital Object Identifier (DOI): 10.53907/enpesj.v6i1.364

Advanced technologies now underpin military readiness, intelligence capabilities, and economic resilience. Yet, unlike earlier strategic technologies, they are overwhelmingly developed and owned by private multinational firms operating in global markets [3]. While states continue to define national priorities, they increasingly depend on privately controlled technologies to implement them. Consequently, private tech firms have become influential non-state actors in global affairs; and states face a reconfiguration of authority and must negotiate and partner with private firms that control critical capabilities. This reality creates new dependencies, redistributes power, and compels states to develop new governance strategies [4].

In this context, diplomacy becomes a tool not only for managing interstate relations but also for engaging the private technology industry in the interest of national security. This situation induces a shift from traditional diplomacy, focused on treaties and state-to-state negotiations, to a new paradigm capable of addressing fast-moving, technically complex, and privately driven innovation ecosystems. This transformation has given rise to new diplomatic practices aimed at coordinating standards, managing technological competition, and fostering cooperation across states, private entities, and international bodies to secure access to critical technologies and shape norms as well as mitigate vulnerabilities. This emerging field, often referred to as technology diplomacy, has become a key mechanism through which states seek to influence the development, diffusion, and governance of critical technologies. Despite the growing importance of technology diplomacy, the relationship between technological competition and diplomatic governance remains insufficiently conceptualized. The existing research often lacks an integrated framework connecting critical technologies to geopolitical competition, diplomatic mechanisms, and global governance. Most analyses focus on state competition (such as US-China rivalry) while the influence of private technology firms remains underexplored, despite their major role in sectors like AI, semiconductors, space telecommunications, and digital infrastructure.

This paper proposes a comprehensive framework for addressing critical technology through tech diplomacy. It first starts by defining the concepts of critical technologies and tech diplomacy. Then the proposed Tech Diplomacy Framework (TDF) is described. As an example of application, the proposed

framework is applied to Low Earth Orbit (LEO) satellite internet which is viewed not as "just space" or "just telecoms" nor as "just internet governance", but as a geopolitical infrastructure that requires dedicated diplomatic capacity.

II. Concepts And Definitions

In this section, we briefly provide the concepts and definitions of critical technologies and Tech Diplomacy.

A. Critical Technologies

A practical approach to comprehend the term "Critical Technologies" (CTs) is to refer to countries' national strategy policies [5]. They are commonly described as advanced technologies that are most significant to achieving national security and are generally termed in ways related to sovereignty and prosperity's are not simply economic assets but strategic resources that are essential for national capabilities and whose control or disruption could significantly affect national interests.

Typically, countries define their CTs on the ground of [6]:

- *Importance to national security and defense:* agencies responsible for defense and intelligence provide input on technologies that need to be protected from foreign threats like espionage, intellectual property theft, and sabotage in key sectors such as energy, communications, finance, and defense;
- *Impact on economic and industrial competitiveness:* governments assess which technologies are vital for maintaining and enhancing their country's economic position. This includes evaluating sectors that contribute to Gross Domestic Product (GDP) growth, job creation, and global competitiveness;
- *Supply chain resilience:* countries consider vulnerability in their supply chains. If technology is reliant on foreign suppliers, especially those from adversarial nations, it is more likely to be considered critical;
- *Global trends and geopolitical considerations:* the CTs' lists are constantly updated in response to new threats, technological advancements, and geopolitical changes. In an era of U.S-China competition, many countries reassess technologies such as AI, advanced semiconductors, and biotechnology to ensure their independence from foreign powers.

CTs often involve cross-border supply chains, international standards, and technology alliances. Countries may impose export controls, investment restrictions, or data protection laws. Therefore, CTs' governance extends beyond domestic policy and enters the realm of diplomacy.

B. Tech Diplomacy

Tech Diplomacy emerged in the 21st century digital era, driven by the geopolitical influence of CTs, technology firms, and digital infrastructures. Its core purpose is to manage technological power relations between states, corporations, and international institutions to shape technology norms and governance. The primary actors include nation-states, private sector technology companies, norms and standards-setting bodies, multi-stakeholder coalitions (such as the UN Tech Envoy and the Global Partnership on AI), academia, and civil society. Its institutional model is based on networked diplomatic architecture operating across states and the private sector. Its main diplomatic logic is based on the recognition that technology embodies geopolitical, ethical, and economic power. Tech diplomacy promotes influence through technological standards, data sovereignty, and leadership in digital governance. Its primary arenas are tech hubs (e.g. Silicon Valley (USA), Shenzhen (China), and Bengaluru (India)); digital summits (e.g., GovTech andIndia-AI Impact), and corporate-state negotiation spaces. Its temporal orientation concerns rapid adaptation to technological disruption, innovation cycles, and global crises. The underlying Philosophy under tech diplomacy is "*Technology for governance and power balance.*" In summary, we define tech diplomacy as:

> "*A technology oriented statecraftto engage governments, international bodies, civil society, andtech industry –spanning the full range of technologies- in order to proactively shape norms, governance and power relations in pursuit of national interests and technological sovereignty."*

A distinctive feature of tech diplomacy is the centrality of private technology firms as strategic actors. As today's critical capabilities are predominantly owned, developed, and operated by private corporations, these firms exercise significant autonomy in shaping technological trajectories, setting industry standards, controlling chokepoints in global supply chains, and making deployment decisions with direct geopolitical consequences [7]. This reconfiguration raises fundamental questions about the distribution of sovereignty in the international order [3] and requires states to develop diplomatic capacities oriented towards corporations that increasingly function as quasi-sovereign actors in the global technology order [8]. Tech diplomacy must therefore engage private firms not simply as regulated entities or procurement partners, but as actors whose decisions (on where to deploy infrastructure, which governments to serve, which standards to adopt, and how to respond to state coercion) constitute acts of political consequence.

C. Related Work and Research Gap

The scholarly literature on technology and international relations has grown substantially, however it remains fragmented across three largely parallel streams: power and statecraft theory [7], [9], interdependence and economic coercion [4], and multi-stakeholder governance [10] [11].

Taken together, these streams illuminate different facets of the technology-diplomacy nexus: power dynamics, structural dependencies, and governance contestation. However, no existing framework integrates these dimensions into a coherent, actionable architecture applicable across different critical technology domains. Moreover, private technology firms, despite their central role in shaping the development, deployment, and governance of critical technologies, remain largely peripheral in both the statecraft and governance literatures. The Tech Diplomacy Framework proposed in Section III aims to fill this gap by offering an integrated, layered model that connects strategic framing, supply chain politics, governance norm-setting, and security management, while explicitly accounting for the growing agency of private sector actors.

III. Proposed Tech Diplomacy framework for addressing Critical Technology

In this section, we propose the Tech Diplomacy Framework (TDF), a comprehensive framework that addresses any critical technology through tech diplomacy. This framework

conceptualizes state engagement with CTs as a layered process that unfolds across four interdependent dimensions: strategic identification and framing, infrastructure and supply chain engagement, technical governance and standards, and security, crisis, and alliance management. It specifies how states should mobilize diplomatic tools across each dimension and offers a cross-domain architecture that connects material, normative, and strategic dimensions into a coherent whole.

This TDF is not tied to specific sectors but instead captures recurring patterns through which states seek to govern, contest, and leverage technological power. It also stresses the role of private technology firms, international bodies, and civil society as actors that states must engage through diplomatic means.

Finally, the proposed framework positions tech diplomacy as a core practice in contemporary international relations (IR) rather than considering it as technical adjunct to foreign policies.

A. Strategic Identification and Framing

The first layer identifies the technologies considered strategically important. Technologies are not designated as critical solely based on their technical characteristics; they are identified as such through sovereignty assessment, economic prioritization, and strategic foresight. Governments classify technologies as critical based on their perceived domestic impacts and strategic geopolitical relevance.

Once specific technologies are deemed critical, policymakers construct narratives linking these CTs to national security and sovereignty, economic competitiveness, and societal resilience, thereby legitimizing extraordinary policy attention and diplomatic engagement. This framing is conveyed through national strategies and foreign policy.

At this stage, tech diplomacy's objective is to understand technological trends and power distribution trajectories by monitoring the global innovation system and assessing technological dependencies through technology foresight programs, science and technology networks, and technology monitoring units in foreign affairs ministries.

B. Infrastructure and Supply-Chain Engagement

CTs' production often involves distributed international value chains that create strategic vulnerabilities in maintaining stable access to technology inputs. Once a technology is framed as critical, tech diplomacy efforts move to the material layer of that technology, where the production networks, logistics systems, physical infrastructures, and transnational supply chains that underpin that technology become central.

Because most advanced technologies rely on globally distributed supply chains, governments must use diplomatic tools to secure access to components, manufacturing capacity, energy, raw materials, technological infrastructures and Intellectual Property. Typically, these resources are unevenly distributed, difficult to substitute in the short term, and often subject to changing policies; as a result, they create asymmetric dependencies that benefit their owners and contribute to what Farrell and Newman describe as infrastructure power [4].

In this layer, tech diplomacy often intersects with industrial policy and economic statecraft, reflecting the blurred boundary between foreign and domestic economic governance. Here, tech diplomacy aims to secure a resilient supply chain and sustain the sourcing of critical inputs (such as raw materials, equipment, and performing hardware). Diplomatic engagement targets allies and suppliers, as well as private firms that control chokepoints in the value chains.

Tech diplomacy actions encompass a range of initiatives, including supply chain diversification policies, supply chain agreements, strategic partnerships, joint manufacturing initiatives, as well as establishing trusted technological partnerships, participating in the technological supply-chain by building regional manufacturing hubs, investing in shared infrastructure projects, and structuring the financial models to access such technologies.

C. Technical Governance and Standards

While standards, protocols, and design choices determine interoperability, scalability, security, and long-term technological trajectories, global technology governance becomes a strategic, diplomatic, and societal imperative [12]. Effective governance aims to align technical and political objectives and turn national interests into interoperable rules.

Here, tech diplomacy operates through sustained engagement with international standards bodies, expert communities, academia, and industry consortia. States deploy diplomats, regulators, engineers, and corporate actors to influence agendas and outcomes, seeking to embed their preferred norms and standards into global systems. This means coordinating across different administrations domestically and participating in global technology governance initiatives, data governance regimes, digital trade agreements, cybersecurity rules and ethical frameworks for emerging technologies.

This layer is particularly significant because technical decisions often precede and constrain later regulatory or political choices, locking advantages for early movers and indirectly shaping global governance. States may seek to export their regulatory models, resist external rules, or construct coalitions around shared governance approaches.

D. Security, Crisis, and Alliance Management

At the strategic layer, critical technologies are integrated into security planning and alliance strategies. Technologies are treated as dual-use capabilities, force multipliers, or vulnerabilities, leading to coordination on protection, denial, or joint development. Tech diplomacy here is often inward-looking toward trusted partners, focusing on alliance cohesion, risk management, and escalation control.

This layer also highlights the growing role of private technology firms as strategic actors whose decisions can affect national security outcomes. Managing public–private interdependence becomes a diplomatic task, reinforcing the need for continuous engagement beyond formal interstate negotiations.

The structure of the proposed technology-agnostic framework allows it to be applied across various domains, such as artificial intelligence and biotechnology to energy systems and space infrastructure. It offers a coherent analytical perspective for understanding how states seek to consolidate their position in a technologically driven international order, in which critical technologies are embedded in sovereignty, development, and privacy.

Taken together, the four layers constitute an integrated diplomatic architecture rather than a sequential checklist. A state's position in any one-layer shapes and constrains its options in the others: a country that fails to frame a technology as strategically critical (Layer 1) will under-invest in supply chain diplomacy (Layer 2), arrive at governance negotiations

without a coherent position (Layer 3), and find itself without pre-negotiated arrangements when a crisis emerges (Layer 4). By contrast, early and thoughtful engagement across all layers can increase advantages. This interdependence is the framework's central analytical claim: tech diplomacy is most effective not when deployed reactively in a single dimension, but when pursued as a coordinated, cross-layer strategy.

A final and cross-cutting dimension of the framework concerns the role of private technology firms. The TDF explicitly positions private firms as co-constitutive actors whose decisions shape outcomes across all four layers. In the strategic framing layer, firms co-produce the narratives and threat assessments that drive governmental classification decisions. In the supply chain layer, corporations controlling critical chokepoints exercise genuine bargaining leverage. In the governance layer, firms engage standards bodies, shape technical architectures, and build coalitions independently, often outpacing governmental processes. Finally, in the security layer, as Starlink's deployment during the war in Ukraine illustrates, private satellite operators can function as de facto strategic actors, making access, coverage, and prioritization decisions with direct military consequences that no existing interstate treaty governs [8]. Tech diplomacy must therefore be understood not only as a state-to-state or state-to-institution practice, but also as a triangular engagement among states, international bodies, and private firms whose structural power increasingly rivals that of sovereign actors in the global technology order [3], [7].

IV. Application: Tech diplomacy applied to space internet

In this section, we apply our proposed framework to address Low Earth Orbit (LEO) satellite internet through Tech diplomacy.

A. Context

As the LEO satellite ecosystem expands, governments must adopt a strategic, security-conscious approach to partnerships. Although services like LEO satellite internet offer transformative potential, they also raise political, economic, and sovereignty risks, such as surveillance and external control. To safeguard digital sovereignty, nations should seek balanced partnerships that ensures equitable, long-term collaboration. These objectives are carried out by tech diplomats, a new breed of IR practitioners.

Addressing satellite internet means addressing the multifaceted legal landscape surrounding this technology [13]. Aspects like services and frequencies licensing (varying from one country to another and presenting diverse requirements for satellite internet providers), cross-border service provisions (involving intricate international laws and agreements[1]) and liability issues (in cases of satellite malfunctions or collisions for instance) call for robust legal frameworks and extensive international cooperation to address these challenges effectively [6]. Moreover, they underscore the necessity for constant dialogue and collaboration between industry players, regulatory bodies, and governments.

Tech diplomats need to participate in developing new international space agreements and work on existing ones as well as establishing norms for good space behaviour. They ought to get involved in regulating access to space and ensure satellite internet activity does not disturb existing scientific and industrial activities like observing comets and meteorites. They are required to address data privacy and security risks, as well as to monitor the dual use of that technology and its militarization due to the growing strategic value of satellite internet for defence and security.

From a technical stance, tech diplomats need to be adequately tooled to comprehend all the implications that result from the adoption of new standards. Furthermore, there is a necessity to address the LEO constellations' environmental impact (such as light pollution and carbon footprint), the constellation protection and disaster recovery, the Critical Space Infrastructure Protection (CSIP), as well as the frequency allocation processes within and across countries. Tech diplomats need to create synergy amongst designers, investors, regulators, manufacturers, and operators to raise awareness on the different impacts [14].

B. TDF applied to LEO Satellite Internet

LEO satellite internet is not "just space," or "just telecoms," nor "just internet governance", but it is a geopolitical infrastructure that requires a dedicated diplomatic approach, as illustrated through the use of our proposed Tech Diplomacy Framework:

Layer 1: Strategic Identification and Framing

Based on its previously addressed challenges and geopolitical aspects, this layer frames LEO satellite internet as a critical technology and a strategic infrastructure, rather than just as a commercial service. Governments should position satellite internet as vital for national resilience, defence readiness, and economic sovereignty. They also need to integrate it into foreign, defence, and development policies while assessing the risks associated with reliance on foreign operators. This translates into:

- Integrating LEO satellite internet into narratives about national security and resilience;
- Reclassifying satellite connectivity as critical or dual-use infrastructure to enable governance across ministries and exceptional regulatory authority;
- Conducting strategic risk assessments related to dependency on foreign-controlled orbital systems, focusing on vulnerability and resilience.

If countries choose not to consider LEO satellite internet as inherently linked to their security, sovereignty, and strategic control, they still need to assess the risks and consequences of this technology, which will affect them directly (due to constellations overflying, space congestion, and potential unauthorized rogue use of the services for instance) as well as indirectly if neighbouring countries use LEO satellite services. Furthermore, they need to consider the governance layer outlined below.

Layer 2: Infrastructure and Supply-Chain Engagement

This layer focuses on the long-term structural dependency of the LEO satellite internet. Unlike terrestrial networks, LEO systems allow foreign providers to deliver essential connectivity within a country without necessarily building or owning significant infrastructure there. This increases the risk of external control over domestic connectivity, which means that decisions about access, pricing, data governance and service continuity may occur beyond national control. Rather than simply facilitating market entry, tech diplomacy emerges here as a mechanism for politically negotiating development outcomes and mitigating

[1]Such as ITU Radio Regulations, WTO and its General Agreement on Trade in Services (GATS) commitments, and Bilateral and Multilateral Agreements.

dependency issues between global satellite operators and host states. The goal is to secure the benefits of LEO satellite internet while avoiding new forms of technological dependency, regulatory weakening, or uneven market power. Diplomatic actions could include negotiating pricing, service coverage and local partnerships while leveraging regional diplomacy and embedding satellite internet in national digital strategies. These objectives can be achieved by:

- Negotiating licensing terms, pricing structures, and coverage obligations;
- Strengthening regional coalitions and leveraging them to improve negotiating power against global operators;
- Advocating for reduced reliance on foreign infrastructure and strategies for mitigating dependency risks;
- Integrating negotiations over LEO satellite connectivity negotiations into broader diplomatic and development strategies;
- Promoting multilateral norms, transparency, and accountability.

Layer 3: Technical Governance and Standards

This layer addresses LEO satellite internet as a case of regime complexity[2] [15], where governance authority spreads across various frameworks of outer space law, international telecommunications regulation, and internet governance. Given that no single institution possesses comprehensive jurisdiction, it creates gaps, inconsistencies, and opportunities for powerful actors.

From a tech diplomacy standpoint, effective governance in such an environment relies on states' ability to coordinate across different regimes, align technical and political objectives, and turn national interests into interoperable rules. Diplomatic efforts should shift from treaty-making toward boundary-spanning practices[3], where technical standards, regulatory procedures, and norms become central instruments of power. Tech diplomacy practices might include:

- Strategic and coordinated diplomatic engagement in multiple institutions (such as the ITU, COPUOS, IGF, IETF and regional regulatory bodies) to avoid contradictory commitments and reduce fragmentation of rules;
- Strategic use of standards-setting and procedural rules to shape market entry, spectrum access, and operational constraints;
- Building coalitions that advocate for the sustainable use of space and for the mitigation of space debris, or countering dominance by early movers and technologically advanced actors;
- Coordinating policies across ministries and agencies (foreign affairs, defense, telecom regulators, and space agencies);
- Translating rules and norms from one governance regime into another. For example, incorporating cybersecurity and data protection concerns into satellite licensing processes.

Layer 4: Security, Crisis, and Alliance Management

As previously noted, during crisis contexts, such as armed conflicts, natural disasters, or state collapse, LEO satellite internet becomes essential for military coordination, humanitarian response, and maintaining government functions. Such situations transform commercial connectivity systems into strategic assets governed through exceptional practices, where typical market logic and regulatory procedures are suspended in favor of ad hoc diplomatic arrangements among states, alliances, and private operators. As private satellite operators become de facto strategic infrastructure providers, pre-negotiated frameworks for emergency access are paramount diplomatic actions to prevent unilateral control over technology. Diplomatic actions should include:

- Negotiating with satellite operators on service prioritization, geographic coverage, and continuity;
- Coordinating with allies to finance, regulate, or substitute commercial services during conflict;
- Developing strategies to reduce dependence on specific providers and enabling multi-vendor strategies on space and terrestrial segments.

When engaging space internet firms, tech diplomats must consider the geopolitical implications of satellite internet access for their countries and the stakes at play with regard to their countries' critical infrastructures, resources and technologies. While seeking to attract Foreign Direct Investments (FDI) inflows, tech diplomats have to ensure that their countries' essential interests are not undermined. They need to pay close attention to the growing race towards launching more LEO satellites that impacts countries' (particularly developing ones) benefit from space access and orbits on the basis of equity.

Table. I

Engaging LEO Satellite internet Companies

Objective	Action
Understanding the industry context and Build collaborative relationships	-Familiarize with companies modus operandi (reliance on spectrum rights, launch infrastructures and global market reach); -Establish open communication channels to discuss licensing, spectrum allocation and national regulatory compliance; -Understand LEO constellations and their implications for global connectivity; -Be aware of international laws, regulations and standards.
Address security and Strategic concerns	-Discuss the implications of LEO satellite networks on national security and emergency communications; -Address concerns around national data sovereignty, cybersecurity and control over critical communications infrastructures; -Address risk mitigation (e.g. working with multiple constellations) and controlling terrestrial segments; -Advocate for cybersecurity measures to protect satellite networks from potential threats.
Advocate for national interest and Facilitate innovation and investment	-Attract investments tied to satellite internet deployment by promoting incentives to invest in local economies through innovation hubs, digital skill training programs, investments in local infrastructure and job creation; -Help streamline regulatory approvals to facilitate market entry while maintaining national interests; -Encourage research and development partnerships between governments, universities and satellite companies to advance innovative technologies.

[2] Governance across overlapping institutions

[3] Diplomatic and governance activities that connect, translate, and coordinate across distinct legal, institutional, and technical domains in order to manage complex technologies that cannot be governed within a single regime.

Table. I- Continued

Engaging LEO Satellite internet Companies

Objective	Action
Leverage international norms and frameworks and Promote ethical and equitable practices	-Encourage regulatory and guidelines compliance; -Engage companies on their plans to mitigate orbital debris and ensure long-term sustainability of space operation; -Incite projects and initiatives that can provide space situational awareness; -Promote LEO satellite internet as a tool for bridging the digital divide; -Address LEO satellite internet firms as key stakeholders in achieving global goals such as universal access under the UN's Sustainable Development Goals (SDGs); -Work with companies to ensure affordable services for marginalized underserved populations.
Act as a bridge between stakeholders	-Connect satellite companies with local telecom providers, communities, and Non-Governmental Organizations (NGOs) to maximize impact; -Facilitate multilateral discussions to harmonize satellite policies and address challenges like signal interference or spectrum management; -Promote synergy between experts, academia and tech companies.

By engaging satellite internet companies, tech diplomats can foster a balanced relationship that promotes technological advancement while safeguarding national and global interests. Table I describes practical actions to effectively engage LEO Satellite internet firms and subtly implies the skillset that tech diplomats need to have.

V. Conclusion

This paper proposes a comprehensive, four-layer analytical and operational Tech Diplomacy Framework (TDF) for addressing CTs through tech diplomacy. The TDF is built around three design principles: it is technology-agnostic, analytically sequential while operationally concurrent, and actor-inclusive. The framework's central analytical claim is that tech diplomacy is most effective when pursued as a coordinated, cross-layer strategy, and that private technology firms must be understood as co-constitutive actors across all four layers.

Low Earth Orbit (LEO) satellite internet was selected as an illustrative use case. This choice was motivated by the multitude of disciplines involved in its development, deployment, and governance (engineering, international relations, law, regulation, and security) and the diverse actors implicated (private entities, governments, and international bodies). This makes it a particularly advocating example for the necessity for international collaboration, sustained by tech diplomacy. A four-layer LEO tech diplomacy framework is provided together with practical actions to effectively engage LEO satellite internet firms, and the skills tech diplomats need.

Future work could extend the Technology Diplomacy Framework (TDF) to other critical technology sectors — such as AI governance or semiconductor supply chains — to further validate its generalizability and develop operationalization metrics that allow states to assess their current diplomatic posture across each layer.

References

[1] D. Archibugi and A. Filippetti, "The retreat of public research and its adverse consequences on innovation," Technological Forecasting and Social Change, vol. 127, pp. 97–111, 2018. https://doi.org/10.1016/j.techfore.2017.05.022

[2] D. Breznitz, C. Dahlman, M. A. Dutz, and B. Hodgson, Making Innovation Policy Work. OECD Publishing/World Bank, 2014. https://doi.org/10.1787/9789264185739-en

[3] M. R. Atal et al., "Oligarchic sovereignty: Technology and the future of global order," Review of International Studies, pp. 1–23, 2025. https://doi.org/10.1017/S0260210525101599

[4] H. Farrell and A. L. Newman, "Weaponized interdependence: How global economic networks shape state coercion," International Security, vol. 44, no. 1, pp. 42–79, 2019. https://doi.org/10.1162/isec_a_00351

[5] M. J. Kim, D. Eom, and H. Lee, "The geopolitics of next-generation mobile communication standardization: The case of Open RAN," Telecommunications Policy, vol. 47, no. 10, p. 102625, 2023. https://doi.org/10.1016/j.telpol.2023.102625

[6] K. D. Remili, N. Bouzourine, R. Hartani, and A. Belouchrani, "Tech diplomacy and critical technologies: Case of LEO satellite internet," Telecommunications Policy, vol. 49, no. 4, p. 102947, 2025. https://doi.org/10.1016/j.telpol.2025.102947

[7] D. W. Drezner, "Technological change and international relations," International Relations, vol. 33, no. 2, pp. 286–303, 2019. https://doi.org/10.1177/0047117819834629

[8] J. Abels, "Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine," European Journal of International Relations, vol. 30, no. 4, pp. 842–866, 2024. https://doi.org/10.1177/13540661241260653

[9] J. S. Nye, Soft Power: The Means to Success in World Politics. New York, NY, USA: PublicAffairs, 2004. ISBN: 978-1-58648-225-1

[10] L. DeNardis, The Global War for Internet Governance. New Haven, CT, USA: Yale University Press, 2014. https://doi.org/10.12987/yale/9780300181357.001.0001

[11] M. L. Mueller, Networks and States: The Global Politics of Internet Governance. Cambridge, MA, USA: MIT Press, 2010. https://doi.org/10.7551/mitpress/9780262014595.001.0001

[12] A. M. Aoki, S. Al Feghali, and E. Garcia, The Global Technology Diplomacy Report 2026. Tech Diplomacy Global Institute, 2026.

[13] M. Pedram and E. Georgiades, "The role of regulatory frameworks in balancing national security and competition in LEO satellite market," Journal of National Security Law and Policy, vol. 14, no. 2, pp. 179–212, 2024.

[14] Y. Chen, X. Ma, and C. Wu, "The concept, technical architecture, applications and impacts of satellite internet: A systematic literature review," Heliyon, vol. 10, no. 13, e33793, 2024. https://doi.org/10.1016/j.heliyon.2024.e33793

[15] K. Raustiala and D. G. Victor, "The regime complex for plant genetic resources," International Organization, vol. 58, no. 2, pp. 277–309, 2004. https://doi.org/10.1017/S0020818304582036