

DIGITAL DIPLOMACY AS AN INSTITUTION OF INTERNATIONAL POLITICAL ECONOMY: THE ECONOMIC POTENTIAL OF OSINT UNDER HYBRID THREATS

Tetiana Krasnopol'ska¹, Yuliia Zavhorodnia², Alina Polukhina³

Abstract. The accelerating digital transformation of international relations has fundamentally reshaped the institutional architecture of diplomacy, expanding its functions far beyond political communication. Contemporary digital diplomacy is increasingly operating as a multidimensional governance mechanism, integrating data infrastructures, artificial intelligence, open-source intelligence (OSINT), digital platforms, and strategic analytics into foreign policy decision-making. Simultaneously, the emergence of hybrid threats has transformed the economic basis of international security, combining military coercion with cyber operations, disinformation, sanctions evasion, technological competition and the manipulation of global supply chains. These developments necessitate a rethink of digital diplomacy, viewing it not merely as a communication tool, but as an institutional component of the international political economy responsible for producing and managing strategic information resources. This article presents a political economy framework that explains how OSINT operates as an economic mechanism within digital diplomacy. Unlike existing studies, which primarily examine OSINT from the perspectives of intelligence, security or investigative journalism, this research conceptualises OSINT as an institutional process that transforms open data into strategic economic information. This information can reduce uncertainty, decrease transaction costs, strengthen sanctions enforcement, improve investment risk assessment and support evidence-based diplomatic decision-making. In terms of methodology, the study draws on political economy, international political economy, institutional economics, digital diplomacy studies, information economics, data economy theory and hybrid threat research. The analytical framework draws on institutional analysis, comparative analysis, document analysis, content analysis, qualitative case studies and OSINT methodology. The article presents an innovative conceptual model that illustrates how hybrid threats drive the institutional development of digital diplomacy by integrating OSINT, data analytics, and strategic decision-making processes. It posits that digital diplomacy has evolved into an institution that generates strategic information capital, thereby bolstering economic security and national competitiveness. The findings contribute to contemporary debates on digital diplomacy by broadening its theoretical interpretation to encompass the political economy of strategic information governance, not just communication and public diplomacy.

Keywords: digital diplomacy, decision-making, foreign policy, OSINT, hybrid threats, economic security, data economy, sanctions, digital governance, transaction costs.

JEL Classification: F50, F51, F52, F53, O33, O38, D80, D83, H56

Received on: June 30, 2026 **Accepted on:** September 27, 2026 **Published on:** October 14, 2026

¹ National University "Odesa Law Academy", Ukraine (*corresponding author*)

E-mail: krasnopolskaya@onua.edu.ua

ORCID: <https://orcid.org/0000-0001-5936-5889>

² National University "Odesa Law Academy", Ukraine

E-mail: zavgorodnaya@onua.edu.ua

ORCID: <https://orcid.org/0000-0003-3500-8638>

³ "GEORGIAN-UKRAINIAN EXPERT CENTER", Ukraine

E-mail: polukhina21@gmail.com

ORCID: <https://orcid.org/0000-0002-3475-448X>



This is an Open Access article, distributed under the terms
of the Creative Commons Attribution CC BY 4.0

1. Introduction

The digital transformation of international relations is one of the most significant institutional changes to affect contemporary diplomacy since the advent of the modern nation-state. Over the past two decades, diplomacy has gradually moved away from a predominantly analogue system of interstate communication towards a digital ecosystem characterised by the exchange of real-time information, algorithmic governance, interaction via platforms, artificial intelligence and an extensive reliance on digital data. Initially seen as an offshoot of public diplomacy on social media, digital diplomacy has evolved into a broad mechanism that supports the formulation of foreign policy, crisis management, international negotiations, the implementation of sanctions, and strategic communication (Bjola & Holmes, 2015; Manor, 2019; Bjola & Manor, 2024).

This transformation has coincided with a fundamental restructuring of the global security landscape. Contemporary interstate competition now encompasses much more than just conventional military confrontation. It increasingly incorporates hybrid instruments, including cyber operations, foreign information manipulation, economic coercion, sanctions circumvention, technological dependence, supply chain disruption and competition over critical digital infrastructures. In this context, information has acquired the characteristics traditionally associated with strategic economic resources. States that can collect, analyse, verify and operationalise digital information have a significant advantage in international political and economic competition. This also reflects the increasing significance of information as an economic asset. Information asymmetry, the quality of information, and the production of knowledge are increasingly determining the effectiveness of institutions and the performance of markets. This reinforces the strategic significance of digital information within the international political economy (Akerlof, 1970; Shapiro & Varian, 1999).

These developments challenge traditional understandings of diplomacy. Existing scholarship predominantly conceptualises digital diplomacy as a means of communication, public engagement, nation branding or digital foreign policy. While these perspectives have advanced our understanding of diplomatic transformation significantly, they only partially explain the increasing integration of diplomacy into contemporary economic governance systems. Digital diplomacy is increasingly performing functions that were traditionally the remit of economic institutions. These include reducing information asymmetries, supporting the implementation of sanctions, facilitating international regulatory coordination, mitigating investment risks, protecting critical infrastructure

and strengthening national economic resilience. This evolution of institutions is consistent with the growing interdependence between information technologies and global governance structures, as described in literature on international political economy (Keohane & Nye, 1998).

At the same time, the rapid proliferation of open-source intelligence (OSINT) has transformed the information underpinnings of diplomatic practice. Advances in satellite imagery, geospatial intelligence, corporate transparency, public procurement databases, maritime and air traffic tracking systems, social media analytics and large-scale open datasets have radically transformed the way governments obtain strategic information. Rather than being used solely for intelligence gathering, OSINT is increasingly being used as a mechanism to support evidence-based diplomatic decision-making within institutions. However, the economic implications of this shift are not yet well understood.

The existing literature has three main limitations.

Firstly, research in the field of digital diplomacy remains largely communication-oriented. It focuses on social media, digital public diplomacy, strategic narratives and government communication online, while paying comparatively little attention to its economic functions within the international political economy.

Secondly, the majority of OSINT scholarship addresses intelligence studies, investigative journalism, conflict documentation and cybersecurity. However, its contribution to areas such as diplomatic governance, economic security, sanctions implementation and international economic coordination has received comparatively little systematic theoretical attention.

Thirdly, although political economy literature extensively examines information asymmetry, institutional governance, transaction costs and digital transformation, it rarely incorporates digital diplomacy as an emerging economic institution that generates strategic informational resources for international decision-making.

Accordingly, this article argues that digital diplomacy should not merely be conceptualised as a technological innovation within foreign policy, but as an evolving institution within the international political economy. Within this institutional framework, OSINT operates as a strategic economic mechanism, transforming dispersed open data into actionable knowledge that bolsters diplomatic effectiveness, economic security and national competitiveness in the face of hybrid threats.

This research aims to develop a political economy framework that explains the institutional relationship between digital diplomacy, open-source intelligence (OSINT), hybrid threats and economic security. More specifically, the study seeks to: (1) conceptualise digital diplomacy as an institution within the international

political economy; (2) identify the economic functions of OSINT within diplomatic governance; (3) analyse how hybrid threats influence the institutional evolution of digital diplomacy; and (4) propose an original conceptual model that links hybrid threats, strategic information production, diplomatic decision-making, economic security and national competitiveness.

The central hypothesis is that digital diplomacy has evolved into an institutional mechanism of the international political economy, producing strategic information capital by integrating OSINT, advanced data analytics and digital governance. This transformation reduces transaction costs, improves the basis for evidence-based foreign policy, strengthens economic security and enhances national competitiveness in conditions of hybrid geopolitical competition.

This article's theoretical contribution lies in its integration of political economy, institutional economics, digital diplomacy and OSINT studies into a unified analytical framework. Unlike existing approaches, which primarily interpret digital diplomacy as a communication practice, this study conceptualises it as a strategic institution that generates economic value by producing, governing and utilising information as a critical economic resource.

2. Materials and Methods

This interdisciplinary study employs a qualitative research design that integrates international political economy, institutional economics, digital diplomacy, information economics, hybrid threat theory and OSINT (Open Source Intelligence). The theoretical interpretation of information as an economic resource draws on contemporary digital economics to explain how digital technologies reshape market structures, institutional governance and public policy (Goldfarb & Tucker, 2019). This theoretical framework conceptualises digital diplomacy as an emerging institution of the international political economy, operating through the governance of strategic information resources.

The analysis is rooted in institutional economics, specifically the theories of North (1990) and Williamson (1985) on how institutions mitigate uncertainty and transaction costs. The analysis combines these concepts with contemporary scholarship on digital diplomacy (Bjola & Holmes, 2015; Manor, 2019; Bjola & Manor, 2024), information economics and hybrid threat studies. The aim is to examine the relationship between digital transformation, diplomatic governance and economic security.

The research takes a qualitative, explanatory approach due to the underdeveloped conceptual understanding of the institutional relationship between digital diplomacy, OSINT and economic security. The analytical framework draws on system analysis,

institutional analysis, comparative analysis, document analysis, content analysis and OSINT methodology. System analysis is used to examine the connections between digital diplomacy, hybrid threats, strategic information and economic governance. Meanwhile, institutional analysis explains how digital technologies are reshaping diplomatic institutions and decision-making processes, and comparative analysis looks at the policy approaches adopted by the European Union, NATO and other democratic states.

The analysis of documentation focuses on strategic documents and policy papers issued by the European Union, the European External Action Service (EEAS), NATO, OECD, and related international organisations. Content analysis is a method of synthesising contemporary academic literature on digital diplomacy, OSINT, institutional economics, and international political economy. Unlike conventional empirical studies, OSINT is examined as both a source of information and an institutional mechanism that supports evidence-based diplomacy, sanctions monitoring, risk assessment and strategic decision-making.

This research's methodological contribution lies in its integration of institutional economics with digital diplomacy studies, explaining how strategic information is transformed into an economic resource. This approach allows digital diplomacy to be analysed as a governance institution that mitigates uncertainty, reduces transaction costs, bolsters economic security and improves national competitiveness in the face of hybrid threats.

3. The Economic Architecture of Digital Diplomacy

The institutional evolution of digital diplomacy has fundamentally altered its functional architecture. While early scholarship primarily associated digital diplomacy with government communication via social media and digital public diplomacy (Bjola & Holmes, 2015; Manor, 2019), more recent research shows that diplomatic institutions are increasingly integrating digital technologies into their strategic governance, organisational adaptation, technological regulation, cybersecurity and foreign policy implementation (Bjola & Manor, 2024). Consequently, digital diplomacy should be understood not as a subsystem of foreign policy, but as a multidimensional governance architecture operating within the digital political economy (Bjola & Manor, 2024).

From an international political economic perspective, institutions perform specific economic functions by reducing uncertainty, coordinating actors, allocating resources and facilitating collective action (North, 1990; Williamson, 1985). This study's findings suggest that digital diplomacy is increasingly performing

these institutional functions through digital infrastructures that support international coordination, economic governance, technological regulation, sanctions implementation and strategic information management. Accordingly, digital diplomacy creates economic value not because it is more efficient than traditional diplomacy, but because it substantially improves governments' institutional capacity to manage information-intensive international environments.

This institutional transformation is indicative of the emergence of what may be termed the economic architecture of digital diplomacy. Unlike traditional diplomatic institutions centred on embassies, negotiations and diplomatic correspondence, digital diplomacy is becoming more dependent on interconnected technological ecosystems comprising digital platforms, cloud infrastructures, artificial intelligence, open data environments, satellite information, cybersecurity systems, algorithmic decision support tools and advanced analytical capabilities. The technological components, when considered collectively, constitute the operational infrastructure through which diplomatic institutions generate strategic value.

The first structural component of this architecture is digital governance. Digital diplomacy is playing an increasingly important role in the development of international norms that regulate cyberspace, cross-border data flows, digital trade, artificial intelligence, digital identity, critical technologies and platform governance. According to Bjola and Manor (2024), diplomatic institutions act as regulatory actors, contributing to the institutional design of the global digital economy rather than merely representing national interests abroad. In this context, digital platforms are increasingly operating as strategic infrastructures through which economic value and political influence are generated. This reflects the broader transformations associated with surveillance capitalism and data-driven governance (Zuboff, 2019).

The second component is economic diplomacy. Contemporary economic diplomacy encompasses more than just trade promotion and investment attraction. It now covers areas such as technological resilience, semiconductor supply chains, investment in digital infrastructure, technological sovereignty, sanctions coordination and international economic security. Digitalisation enables governments to respond more rapidly to disruptions in global markets while strengthening coordination among allies through shared digital infrastructures.

The third component is data diplomacy. As governments increasingly recognise data as a strategic economic asset, diplomatic activity has expanded to include negotiations on rules governing cross-border data transfers, digital sovereignty, data protection, interoperability standards and digital public goods.

In this context, diplomatic negotiations are increasingly concerned with access to information resources rather than physical markets alone. Consequently, information governance has become an important dimension of the international political economy.

The fourth component is technology diplomacy, which reflects the increasing geopolitical importance of new technologies. An increasing number of ministries of foreign affairs are establishing specialised units responsible for artificial intelligence governance, quantum technologies, semiconductors, biotechnology, cybersecurity and digital innovation. Consequently, technology diplomacy represents an institutional response to the technological competition between major powers, particularly with regard to critical technologies that have economic and security implications (Bjola & Manor, 2024).

The fifth component is cyber diplomacy, which involves international co-operation on issues such as cyber resilience, cyber norms, cyber deterrence and the protection of critical digital infrastructure. As cyberattacks directly affect financial markets, supply chains, payment systems, transportation networks, and energy infrastructure, cyber diplomacy increasingly intersects with economic diplomacy. Correspondingly, cybersecurity is not only a security issue, but also an essential element of economic governance.

Drawing upon these observations, this article identifies OSINT as the sixth structural component of the economic architecture of digital diplomacy. Existing literature predominantly analyses OSINT within intelligence studies, investigative journalism, or cybersecurity. However, the findings presented here suggest that OSINT performs a broader institutional function. It provides diplomatic institutions with continuously updated evidence to support the implementation of sanctions, economic risk assessment, strategic communication, investment analysis, technology governance, and international negotiations.

Unlike classified intelligence, OSINT operates within environments where information is legally accessible. Collectively, satellite imagery, corporate ownership registers, customs databases, procurement platforms, financial disclosures, maritime tracking systems, aviation databases, scientific publications, patent databases, social media and geospatial information provide governments with unprecedented opportunities for evidence-based diplomacy. These information ecosystems are economically significant because they can reduce informational uncertainty and improve institutional responsiveness in rapidly changing geopolitical conditions.

Integrating OSINT into digital diplomacy also transforms the economics of diplomatic decision-making. Traditionally, diplomatic analysis relied on lengthy reporting procedures, fragmented institutional communication and limited accessibility of information.

Digital diplomacy, supported by OSINT, has been demonstrated to substantially reduce information acquisition costs while simultaneously increasing analytical speed, transparency, and adaptability. From the perspective of institutional economics, these developments contribute directly to lowering transaction costs associated with strategic decision-making (North, 1990; Williamson, 1985).

The analysis conducted in this study therefore supports the proposition that digital diplomacy creates a new category of strategic resource, which is referred to here as 'strategic information capital'. Unlike conventional information assets, strategic information capital emerges from the institutional integration of digital infrastructures, analytical capabilities, technological governance and diplomatic expertise. Its economic value does not derive from information abundance itself, but from the state's institutional capacity to convert dispersed digital information into reliable diplomatic knowledge that supports foreign policy and economic governance.

Accordingly, the economic architecture of digital diplomacy may be conceptualised as an integrated institutional system comprising six mutually reinforcing dimensions: digital governance, economic diplomacy, data diplomacy, technology diplomacy, cyber diplomacy, and OSINT-enabled strategic analytics. Together, these dimensions transform diplomacy from a communication-oriented institution into a mechanism that generates strategic information capital for the international political economy. This proposed interpretation builds upon existing scholarship in digital diplomacy by introducing an institutional political economy perspective. The present study demonstrates that digital diplomacy should not be viewed primarily through the lens of communication technologies. Instead, its principal economic function lies in governing strategic information resources capable of enhancing economic security, institutional resilience, regulatory coordination, and national competitiveness under conditions of hybrid geopolitical competition.

4. OSINT as the Information-Analytical Mechanism of Digital Diplomacy

The rapid expansion of publicly accessible digital information has fundamentally transformed the informational foundations of diplomatic activity. Governments no longer rely solely on classified intelligence or traditional diplomatic reporting to evaluate international developments. Instead, diplomatic institutions are increasingly integrating publicly available digital information into their strategic decision-making processes, thereby enhancing the analytical capabilities of foreign ministries and other government agencies (Bjola &

Manor, 2024). Traditionally, OSINT (Open Source Intelligence) has been associated with the intelligence community, military analysis, investigative journalism and cybersecurity. Scholarship in this area generally defines OSINT as the systematic collection, verification, analysis and interpretation of information that is legally accessible and obtained from publicly available sources. These sources include government databases, corporate registries, customs records, satellite imagery, maritime and aviation tracking systems, social media platforms, scientific publications, patent databases, geospatial information and financial disclosures (NATO, 2024; OECD, 2024).

Although this understanding accurately reflects the operational aspect of OSINT, it only partially explains why it is becoming increasingly important within the field of international political economy. The present study indicates that the primary significance of OSINT lies not in information collection itself but in its capacity to transform fragmented digital information into evidence supporting diplomatic governance. Consequently, OSINT should be understood as an institutional analytical mechanism embedded within digital diplomacy rather than as an autonomous intelligence discipline.

This distinction is of particular importance given the fundamental difference between diplomatic decision-making and intelligence operations. Intelligence organisations primarily seek to reduce strategic uncertainty for national security purposes, whereas diplomatic institutions require analytically verified information capable of supporting negotiations, international regulatory coordination, sanctions implementation, economic co-operation, crisis management, and strategic communication. Within this institutional environment, OSINT functions as the analytical interface connecting digital information ecosystems with diplomatic governance. Analytical approaches of a similar nature are being used with increasing frequency to identify networks of sanctions evasion and illicit financial flows associated with proliferation financing (Financial Action Task Force, 2025).

The institutional integration of OSINT has been demonstrated to have a significant impact on the production of diplomatic knowledge. Conventional diplomatic reporting is predicated on hierarchical communication channels, official correspondence, and confidential governmental exchanges. Despite the continued indispensability of these mechanisms, they are increasingly complemented by continuous monitoring of open digital environments. Satellite observations, customs statistics, commercial shipping databases, public procurement systems, corporate ownership records, and digital platform analytics provide diplomatic institutions with independent sources for verifying official information and identifying

emerging geopolitical and economic trends (Bjola & Manor, 2024). From the perspective of institutional economics, this transformation substantially reduces information-related transaction costs. North (1990) posits that institutions are formed to mitigate uncertainty by organising interactions among actors, while Williamson (1985) underscores the significance of reducing transaction costs associated with information acquisition, monitoring, and coordination. Digital diplomacy, supported by OSINT, contributes directly to these objectives by accelerating access to verified information, facilitating cross-institutional coordination, and reducing analytical duplication across governmental agencies.

The significance of OSINT in the implementation of international sanctions is particularly pronounced. Since 2022, democratic states have increasingly relied on open-source analytical methods to identify sanctions circumvention schemes, monitor dual-use goods, analyse corporate ownership structures, trace maritime transportation routes, and detect modifications in international supply chains. The European Union has progressively strengthened its co-operation with regard to export controls and the identification of items that could contribute to Russia's military-industrial capabilities (European Commission, 2024a, 2024b). In this context, OSINT allows diplomatic institutions to conduct evidence-based consultations with partner governments and international organisations on sanctions enforcement and export control mechanisms.

A second strategic function of OSINT is economic risk assessment. Contemporary diplomatic institutions are increasingly involved in analysing geopolitical risks that affect investment environments, technological co-operation, energy security and the resilience of critical infrastructure. Unlike traditional macroeconomic indicators, OSINT allows governments to identify early signs of political instability, technological disruption, changes to logistics, or regulatory shifts by continuously monitoring digital information ecosystems. As a result, diplomatic risk assessment becomes more dynamic and evidence-based.

The growing importance of OSINT also reflects broader changes in the global data economy. Information has become an economic asset whose value depends not only on its availability, but also on institutional capacities for verification, integration and interpretation. Accordingly, diplomatic institutions that can efficiently process open-source information gain a competitive edge in international negotiations, regulatory co-operation, technological governance and crisis response. This observation lends weight to the central argument of the present study, which is that strategic information should be conceptualised as a form of institutional capital rather than merely an operational resource.

Based on these findings, this article introduces the concept of OSINT-enabled diplomatic intelligence. This refers to the institutional capability of diplomatic organisations to transform legally accessible digital information into verified analytical knowledge that supports the formulation of foreign policy, international economic governance and strategic decision-making. Unlike conventional intelligence, OSINT-enabled diplomatic intelligence operates within transparent legal frameworks, deriving its legitimacy from methodological verification rather than informational secrecy.

The empirical evidence reviewed throughout this study further demonstrates that the effectiveness of OSINT hinges on its integration with other analytical capabilities. Open-source information alone rarely provides a solid basis for strategic decisions. It is only through systematic validation, cross-referencing, contextual interpretation and incorporation into broader diplomatic and economic analyses that its practical value emerges. Consequently, OSINT should be understood as just one component of a broader analytical ecosystem encompassing artificial intelligence, geospatial analysis, data analytics, institutional expertise and diplomatic judgement.

The results of the present study suggest that OSINT represents the analytical core of contemporary digital diplomacy. Instead of replacing established diplomatic practices, it enhances institutional capacities by empowering governments to respond more swiftly to hybrid threats, technological competition, sanctions circumvention, economic coercion, and information manipulation. By doing this, OSINT directly contributes to the creation of strategic information capital, thereby reinforcing the institutional capacity of digital diplomacy to function as an integral part of the international political economy.

In summary, the present analysis demonstrates that OSINT performs four interrelated institutional functions within digital diplomacy: informational, by expanding access to strategically relevant data; analytical, by transforming raw information into evidence-based knowledge; economic, by reducing transaction costs and improving policy efficiency; and governance, by strengthening coordination among diplomatic institutions engaged in international economic and security co-operation. Collectively, these functions position OSINT not as an auxiliary technology but as one of the principal analytical mechanisms underpinning the institutional evolution of digital diplomacy in the twenty-first century.

5. Hybrid Threats as a Driver of Digital Diplomacy Transformation

The institutional transformation of digital diplomacy must be understood in relation to the changing

geopolitical environment. The increasing prevalence of hybrid threats has had a profound impact on the priorities, organisational structures and operational mechanisms of diplomatic institutions. Rather than functioning solely as instruments of political representation and interstate communication, ministries of foreign affairs are increasingly operating within complex digital ecosystems. In these ecosystems, cyber resilience, technological governance, strategic communication, sanctions coordination and information integrity are all integral components of foreign policy (EEAS, 2023; Bjola & Manor, 2024).

Hybrid threats differ from conventional security challenges in that they deliberately combine military and non-military instruments to exploit political, economic, technological, informational, and societal vulnerabilities. Hybrid threats differ from conventional security challenges in that they deliberately combine military and non-military instruments to exploit political, economic, technological, informational, and societal vulnerabilities. In the European Union's policy discourse, hybrid threats are understood as complex cross-domain activities that combine cyber operations, disinformation, economic coercion, sabotage, technological interference, and political influence in order to undermine democratic institutions and social resilience without necessarily crossing the threshold of conventional armed conflict (Council of the European Union, 2026; NATO, 2024).

In this environment, digital diplomacy has evolved from a communication-oriented activity into an institutional mechanism that supports resilience against hybrid threats. The 2023 Council Conclusions on EU Digital Diplomacy and the subsequent EU International Digital Strategy emphasise that digital diplomacy should strengthen the European Union's strategic autonomy while simultaneously promoting an open, secure, and rules-based digital order. These developments are further reflected in the Council Conclusions on EU Digital Diplomacy, which recognise digital diplomacy as an essential component of the European Union's external action and strategic autonomy (Council of the European Union, 2023). Consequently, digital diplomacy increasingly incorporates cybersecurity, digital governance, technological partnerships, artificial intelligence, and international regulatory co-operation into its external action. Recent Council conclusions on the future of EU digital policy further emphasise the strategic importance of secure digital infrastructures, trusted technologies, and coordinated governance mechanisms (Council of the European Union, 2024).

The findings of this study indicate that hybrid threats generate four interconnected institutional transformations within digital diplomacy.

The first transformation relates to the expansion of diplomatic functions. Diplomatic institutions are no longer solely responsible for political dialogue.

They are increasingly involved in coordinating cyber resilience, technological standards, the implementation of sanctions, countermeasures against foreign information manipulation, the protection of digital infrastructure, and supply-chain security. The European Union's contemporary digital diplomacy explicitly links these policy areas within a coherent external digital strategy.

The second transformation is the increasing importance of strategic information governance. Information has become a strategic asset, the control of which directly affects geopolitical influence and economic competitiveness. Campaigns of Foreign Information Manipulation and Interference (FIMI) illustrate how state and non-state actors deliberately manipulate digital information environments in order to influence public opinion, weaken institutional trust and shape international decision-making processes. Recent assessments by the European External Action Service (EEAS) indicate that coordinated foreign information manipulation campaigns are increasingly combining cyber activities, digital platforms and economic narratives in order to influence democratic decision-making processes (EEAS, 2025). In response, the European Union has developed institutional instruments, including the FIMI Toolbox, the Rapid Alert System, the EU Cyber Diplomacy Toolbox and the European Digital Media Observatory, which integrate strategic communication with diplomatic action.

The third transformation relates to economic security. Hybrid threats are increasingly targeting economic infrastructure rather than military capabilities exclusively. This includes supply chains, semiconductor production, digital platforms, energy systems, financial networks and critical technologies, all of which have become the focus of geopolitical competition. Consequently, diplomatic institutions are playing an increasingly important role in building economic resilience by supporting technological partnerships, coordinating export controls, strengthening the implementation of sanctions, and facilitating international co-operation on the protection of critical infrastructure. Digital diplomacy thus plays a significant role in economic governance, extending far beyond traditional diplomatic communication.

The fourth transformation relates to evidence-based diplomacy. In the context of hybrid competition, the credibility of diplomacy is increasingly dependent on the availability of verifiable evidence. Rather than merely communicating political positions, governments are expected to substantiate them with reliable analytical information. This development has greatly increased the importance of OSINT, satellite imagery, corporate transparency data, customs statistics, geospatial analysis and other open-source analytical methods. Therefore, the ability to transform dispersed digital information into diplomatically credible evidence has become

a defining characteristic of contemporary digital diplomacy.

Collectively, these transformations demonstrate that hybrid threats act as an institutional catalyst rather than merely an external security challenge. They accelerate organisational adaptation within ministries of foreign affairs, encourage closer co-operation between the diplomatic and intelligence communities, stimulate technological innovation and reinforce the integration of digital governance within the international political economy.

Based on these observations, this study suggests that hybrid threats create a demand within institutions for strategic information. As geopolitical competition increasingly takes place within digital environments, governments require the continuous production of verified analytical knowledge to support rapid diplomatic responses. Strategic information capital thus becomes an essential economic resource and institutional prerequisite for effective digital diplomacy.

This interpretation differs from conventional security-oriented analyses in one key respect. Existing studies typically treat hybrid threats as external drivers of policy adaptation. In contrast, the present research argues that hybrid threats also reshape the internal institutional architecture of diplomacy. They redefine diplomatic competencies, expand analytical capacities, strengthen interagency coordination and transform information governance into a core foreign policy function.

Consequently, the relationship between hybrid threats and digital diplomacy should be understood as reciprocal rather than linear. The advent of hybrid threats has given rise to the institutional evolution of digital diplomacy. Digital diplomacy, in turn, has enhanced the capacity of states to anticipate, analyse, communicate, and mitigate hybrid threats through coordinated international action. This reciprocal interaction establishes the institutional foundation upon which OSINT, data analytics, and artificial intelligence collectively generate strategic information capital capable of strengthening economic security and national competitiveness within the contemporary international political economy.

6. The Political and Economic Implications of Using OSINT in Digital Diplomacy

As demonstrated in the previous sections, digital diplomacy has evolved beyond its traditional communicative functions to increasingly operate as an institutional mechanism for governing strategic information. Within this institutional framework, OSINT should not merely be viewed as a technical method of gathering publicly accessible information. Instead, it is an economic mechanism that generates

measurable value through the production of verified analytical knowledge supporting diplomatic governance, international economic coordination, and evidence-based foreign policy (North, 1990; Williamson, 1985; Bjola & Manor, 2024). From the perspective of political economy, the principal economic value of OSINT derives from its ability to reduce uncertainty. Uncertainty is recognised as a primary cause of inefficiency in both markets and political decision-making. In circumstances where governments are operating under conditions of incomplete or asymmetric information, additional costs are frequently incurred. These additional costs are associated with delayed responses, policy errors, inefficient resource allocation and ineffective international coordination. The continuous integration of information from legally accessible digital sources has been demonstrated to substantially improve the informational environment within which diplomatic institutions formulate strategic decisions.

This research argues that the economic effects of OSINT can be best understood by considering four interconnected dimensions: informational efficiency, institutional efficiency, strategic efficiency and competitive efficiency. Together, these dimensions explain why OSINT has become an indispensable part of modern digital diplomacy.

The first dimension is informational efficiency. In an increasingly digital world, diplomacy depends on having timely access to reliable information about geopolitical developments, sanctions regimes, technological innovation, supply-chain disruptions, investment risks and foreign information manipulation. Unlike traditional diplomatic reporting, which often relies on hierarchical communication channels and confidential exchanges, OSINT allows for the continuous monitoring of dynamic digital environments. As a result, diplomatic institutions can identify emerging risks before they escalate into political or economic crises (Bjola & Holmes, 2015; Bjola, 2019; Manor, 2019).

The second dimension concerns institutional efficiency. According to institutional economics, governance systems create value by reducing the transaction costs associated with acquiring information, monitoring, coordinating and enforcing (North, 1990; Williamson, 1985). The empirical analysis conducted in this study indicates that integrating OSINT into diplomatic institutions substantially improves their performance. Ministries of Foreign Affairs are increasingly relying on digital analytical platforms, geospatial intelligence, corporate transparency databases, customs information and publicly accessible economic indicators to support policy coordination across government agencies. Consequently, diplomatic institutions reduce the duplication of analytical work, thereby improving interagency co-operation and decision-making speed.

The third dimension is strategic efficiency. In the contemporary world, foreign policy increasingly requires governments to respond simultaneously to cyber incidents, economic coercion, sanctions circumvention, technological competition and rapidly evolving geopolitical crises. These dynamics are closely associated with the growing importance of soft power and information influence in shaping international political and economic relations (Nye, 2004). In such circumstances, the value of information hinges more on its credibility, timeliness and analytical integration than on its exclusivity. OSINT allows diplomatic institutions to convert scattered digital data into evidence that can support negotiations, sanctions enforcement, international advocacy and crisis diplomacy. This process has strategic significance that extends beyond intelligence gathering because it directly affects diplomatic credibility and policy legitimacy.

The fourth dimension is competitive efficiency. International competitiveness is increasingly dependent on institutional capabilities rather than material resources alone. Those states with advanced analytical capabilities are better placed to anticipate geopolitical risks, identify technological opportunities, strengthen regulatory co-operation and foster international economic partnerships. Therefore, the competitive advantage generated by digital diplomacy does not arise from technological sophistication alone, but from the institutional ability to transform information into strategic economic decisions.

Based on these observations, this article introduces the concept of the Political-Economic Value Chain of Digital Diplomacy. Unlike linear models, which portray diplomacy as a sequence of communication activities, the proposed framework conceptualises diplomatic governance as a process of economic value creation through the strategic management of information.

The proposed value chain comprises six sequential stages.

The first stage involves the emergence of hybrid threats, which create strategic uncertainty within the international system. Examples of these threats include cyber operations, economic coercion, technological dependencies, foreign information manipulation, sanctions circumvention and disruption to global supply chains.

The second stage involves systematically acquiring open-source information through OSINT. Here, governments collect information from sources such as satellite imagery, customs databases, corporate registries, scientific publications, maritime and aviation tracking systems, and digital platforms.

The third stage is analytical integration, where raw information is verified, cross-referenced, interpreted and transformed into structured knowledge. The findings of this research suggest that this stage

is the main source of economic value creation, as information only acquires strategic significance after analytical validation.

The fourth stage involves digital diplomatic decision-making. Verified analytical knowledge underpins international negotiations, the implementation of sanctions, export control policies, investment screening, technological partnerships, strategic communication and diplomatic coordination with international organisations.

The fifth stage focuses on economic security outcomes. The effective diplomatic use of strategic information can help to reduce geopolitical uncertainty, strengthen sanctions compliance, protect critical infrastructure, improve supply-chain resilience, support regulatory co-operation and enhance investor confidence. Finally, the sixth stage results in national competitiveness. Governments that can systematically integrate strategic information into diplomatic governance develop stronger institutional resilience, greater policy adaptability, improved technological co-operation and enhanced international credibility.

The analysis in this study therefore suggests that OSINT should be understood as a productive institutional asset, rather than just an analytical tool. Similar to financial or technological capital, the strategic information generated through OSINT improves the quality of governance under conditions of uncertainty, thereby contributing to long-term state capacity.

One important implication of these findings is the changing nature of diplomatic resources. Traditional diplomacy relied primarily on diplomatic networks, confidential correspondence and political expertise. In contrast, contemporary digital diplomacy increasingly depends on institutional capabilities to acquire, validate, integrate and operationalise digital information. Consequently, information itself becomes an economically productive diplomatic resource, the value of which depends on institutional governance rather than informational scarcity.

Based on these findings, the article proposes the following definition:

Strategic Information Capital refers to a state's institutional capacity to systematically transform verified digital information into evidence-based diplomatic knowledge, thereby generating sustainable political and economic value. This knowledge supports international decision-making, economic security, and national competitiveness.

Unlike existing approaches, which interpret digital diplomacy primarily in terms of communication technologies or public diplomacy, this study shows that its main contribution is the generation of strategic information capital. OSINT is the analytical mechanism through which this capital is produced, and digital diplomacy provides the institutional environment in which it is transformed into foreign policy outcomes.

Accordingly, the political and economic significance of OSINT goes far beyond intelligence analysis. It directly contributes to reducing institutional uncertainty, strengthening economic governance, improving diplomatic effectiveness, supporting international regulatory coordination and enhancing national resilience against hybrid threats. These findings reinforce the central argument of this article, which is that digital diplomacy should be conceptualised as an institution of the international political economy. The most valuable resource of this institution is not digital communication itself, but rather the production and governance of strategic information capital.

7. An Integrated Conceptual Model of Digital Diplomacy within International Political Economy

The preceding analysis shows that digital diplomacy cannot be adequately explained by communication-oriented models that focus on social media engagement or digital public diplomacy alone. Rather, the institutional changes observed in democratic states suggest the development of a much broader governance framework, in which diplomatic institutions coordinate information, technology, regulation and economic security simultaneously (Bjola & Holmes, 2015; Manor, 2019; Bjola & Manor, 2024).

Despite significant advances in the research of digital diplomacy, existing theoretical approaches generally examine the various components of this transformation in isolation. Studies of digital diplomacy primarily analyse diplomatic communication and organisational adaptation. Information economics focuses on the economic value of information, while institutional economics explains governance through transaction-cost reduction. OSINT literature, meanwhile, concentrates on intelligence methodologies. To date, there has been a paucity of attention devoted to the integration of these perspectives into a unified political economy framework. Such a framework would be required to explain how strategic information generates economic value through diplomatic institutions.

In order to address this gap, this study proposes an integrated conceptual model that explains the institutional production of strategic information capital under conditions of hybrid geopolitical competition.

Hybrid Threats → Digital Diplomacy → OSINT and Advanced Analytics → Strategic Diplomatic Knowledge → Economic Security → National Competitiveness

In contradistinction to prevailing linear interpretations, the proposed model conceptualises digital diplomacy as the institutional environment within which strategic information is transformed into political and economic value. The model thus places greater emphasis on institutional interaction than on technological determinism.

Stage 1. Hybrid Threats as Institutional Drivers

Hybrid threats form the basis of the model. In the contemporary geopolitical landscape, competition increasingly combines military force with cyber operations, technological dependence, economic coercion, sanctions circumvention, foreign information manipulation, interference in critical infrastructure and disruption to global supply chains. These developments generate persistent strategic uncertainty and increase the demand among governments for reliable analytical information.

Accordingly, hybrid threats should not be interpreted solely as external security challenges. Instead, they act as drivers of institutional change, stimulating organisational adaptation within diplomatic systems by increasing the need for continuous information acquisition, verification and strategic analysis.

Stage 2. Digital Diplomacy as Institutional Infrastructure

The second stage involves the institutional architecture through which governments organise their responses to hybrid threats. Digital diplomacy provides an organisational framework that connects ministries of foreign affairs, economic institutions, cybersecurity agencies, regulatory authorities, international organisations and strategic partners via digital governance mechanisms.

Within this framework, diplomacy plays a much broader role than traditional interstate representation. Its remit includes coordinating technological co-operation, implementing sanctions, enhancing cyber resilience, promoting digital governance, protecting investment, ensuring supply-chain security, and facilitating international regulatory dialogue.

Consequently, digital diplomacy acts as the institutional framework for managing strategic information, rather than simply communicating government positions.

Stage 3. OSINT and Advanced Analytical Capacity

The third stage consists of systematic production of verified knowledge through OSINT integrated with advanced analytical methods.

The analytical process includes:

- Collection of legally accessible digital information;
- verification through multiple independent sources;
- geospatial and temporal analysis;
- integration of economic, political, technological, and security indicators;
- analytical interpretation supporting diplomatic decision-making.

Crucially, the model assumes that information itself does not generate economic value. Strategic value only emerges after information has undergone institutional verification and analytical interpretation.

Accordingly, OSINT should be considered an institutional knowledge production mechanism rather than just an intelligence technique.

Stage 4. Strategic Diplomatic Knowledge

The fourth stage represents the central value-creation process.

This study suggests that diplomatic institutions are increasingly producing strategic diplomatic knowledge. This is defined as information that has been analysed and validated, and which can support international negotiations, the implementation of sanctions, technological co-operation, crisis management, regulatory coordination and the formulation of foreign policy.

This distinction is important in theory because it separates raw digital information from institutional knowledge. Open-source information has limited practical significance until it is transformed into analytically verified evidence and incorporated into diplomatic decision-making processes.

Therefore, the main outcome of the institutional interaction between digital diplomacy and OSINT is strategic diplomatic knowledge.

Stage 5. Economic Security

The fifth stage focuses on the practical implications of evidence-based diplomatic governance.

The analysis conducted in this study suggests that strategic diplomatic knowledge can contribute to economic security via several interconnected mechanisms.

Firstly, it reduces information asymmetry, which influences the government's decision-making process.

Secondly, it enhances the effectiveness of sanctions and the implementation of export control policies.

Thirdly, it strengthens the resilience of critical infrastructure by enabling the early identification of technological and geopolitical vulnerabilities.

Fourthly, it facilitates more informed strategic investment decisions through improved assessment of geopolitical risks.

Finally, it facilitates international regulatory coordination concerning digital technologies, cybersecurity, artificial intelligence, and data governance.

Together, these mechanisms demonstrate that digital diplomacy is becoming an important contributor to economic governance, rather than operating exclusively within the political sphere.

Stage 6. National Competitiveness

The final stage is the overall result of the institutional process.

National competitiveness should not be interpreted solely in terms of macroeconomic indicators such as productivity, exports or technological innovation. In the context of digital transformation, a country's ability to generate, govern and operationalise strategic information is becoming an increasingly important factor in its competitiveness.

Countries that can integrate digital diplomacy, OSINT, advanced analytics and evidence-based

policymaking are better placed to anticipate geopolitical risks, strengthen international partnerships, attract investment, safeguard technological sovereignty and respond effectively to hybrid threats.

Accordingly, strategic information capital has become an additional factor in determining national competitiveness within the contemporary international political economy.

Theoretical Implications of the Model

The proposed model expands the scope of existing academic research in several respects:

Firstly, it redefines digital diplomacy as an institution of international political economy, rather than merely as a communicative practice.

Secondly, it integrates OSINT into the institutional architecture of diplomacy, rather than treating it as a standalone intelligence activity.

Thirdly, it explains how verified digital information is transformed into strategic diplomatic knowledge capable of generating measurable political and economic value.

Fourthly, it introduces the concept of 'strategic information capital' as a conceptual category describing the institutional capacity to transform digital information into sustainable diplomatic, economic and strategic advantages.

Rather than replacing existing theories of digital diplomacy, the proposed framework integrates institutional economics, information economics, international political economy and digital diplomacy to provide a coherent analytical perspective. By doing so, it establishes a basis for examining diplomacy as a productive institution operating within the global digital economy, in which information governance has become an increasingly important source of state power, economic resilience and international competitiveness.

8. Conclusions

Digital diplomacy has evolved from communication and public diplomacy to become an institutional mechanism of the international political economy. OSINT is a key analytical tool of digital diplomacy, transforming open digital data into evidence-based diplomatic knowledge. The increased threat of hybrid warfare is creating a greater demand for verified information, strategic analytics and coordinated digital diplomatic responses. The economic value of OSINT lies in its ability to reduce uncertainty, lower transaction costs, improve sanctions enforcement and support risk assessment. Digital diplomacy strengthens economic security by linking information governance, technological resilience, sanctions policy and international coordination. The concept of Strategic Information Capital explains how states generate political and economic value through verified

digital information. The study shows that a country's competitiveness is increasingly dependent not only on material resources, but also on its ability to manage

strategic information. Future research should develop quantitative indicators to measure the economic impact of OSINT-based digital diplomacy.

References:

- Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3), 488–500. <https://doi.org/10.2307/1879431>
- Bjola, C. (2019). The dark side of digital diplomacy: Countering disinformation and propaganda. *Real Instituto Elcano*. <https://www.realinstitutoelcano.org/en/analyses/the-dark-side-of-digital-diplomacy-countering-disinformation-and-propaganda/>
- Bjola, C., & Holmes, M. (Eds.). (2015). *Digital diplomacy: Theory and practice*. Routledge. <https://doi.org/10.4324/9781315730844>
- Bjola, C., & Manor, I. (Eds.). (2024). *The Oxford handbook of digital diplomacy*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.001.0001>
- Council of the European Union. (2023). Council conclusions on EU digital diplomacy (11088/23). <https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf>
- Council of the European Union. (2024). The future of EU digital policy: Council conclusions (9957/24). <https://data.consilium.europa.eu/doc/document/ST-9957-2024-INIT/en/pdf>
- Council of the European Union. (2026). Hybrid threats. <https://www.consilium.europa.eu/en/policies/hybrid-threats/>
- European Commission. (2024a). List of common high priority items. https://finance.ec.europa.eu/publications/list-common-high-priority-items_en
- European Commission. (2024b). EU and partners expand list of common high priority items to further weaken Russia's war effort. https://policy.trade.ec.europa.eu/news/eu-and-partners-expand-list-common-high-priority-items-further-weaken-russias-war-effort-2024-02-23_en
- European External Action Service. (2023). Digital diplomacy for a secure and competitive Europe. https://www.eeas.europa.eu/eeas/digital-diplomacy-secure-and-competitive-europe_en
- European External Action Service. (2025). 3rd EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats_en
- Financial Action Task Force. (2025). Complex proliferation financing and sanctions evasion schemes. FATF/OECD. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf>. [coredownload.inline.pdf](https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf)
- Goldfarb, A., & Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, 57(1), 3–43. <https://doi.org/10.1257/jel.20171452>
- Keohane, R. O., & Nye, J. S. (1998). Power and interdependence in the information age. *Foreign Affairs*, 77(5), 81–94. <https://doi.org/10.2307/20049052>
- Manor, I. (2019). *The digitalization of public diplomacy*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-04405-3>
- North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge University Press.
- North Atlantic Treaty Organization. (2024). NATO's approach to countering hybrid threats. <https://www.nato.int/https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats>
- Nye, J. S. (2004). Soft power: The means to success in world politics. PublicAffairs. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/joe_nye_wielding_soft_power.pdf
- Organisation for Economic Co-operation and Development. (2024). *OECD digital economy outlook 2024*. OECD Publishing. <https://doi.org/10.1787/b9a84b44-en>
- Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy*. Harvard Business School Press.
- Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting*. Free Press.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.