ISRG Journal of Multidisciplinary Studies (ISRGJMS)

ISRG PUBLISHERS

Abbreviated Key Title: isrg j. multidiscip. Stud.

ISSN: 2584-0452 (Online)

Journal homepage: https://isrgpublishers.com/isrgjms/

Volume – IV, Issue – VII (July) 2026

Frequency: Monthly

From Digital Sovereignty to Data-Driven Power Architecture: How Artificial Intelligence, Cybersecurity, and Global Governance Are Transforming the International System

Dr. Sıddık Arslan

Deputy Secretary General of Erzurum Metropolitan Municipality, Türkiye.

| **Received:** 15.06.2026 | **Accepted:** 21.06.2026 | **Published:** 12.07.2026

***Corresponding author:** Dr. Sıddık Arslan

Abstract

This study examines, within an interdisciplinary framework, how digital technologies are transforming international relations in the domains of security, economics, and diplomacy. It treats developments in artificial intelligence, blockchain, quantum computing, and cybersecurity not as separate technical innovations but as interconnected processes that reconfigure states' power capacities and their relations of interdependence. A qualitative and interpretive method is adopted, combining a review of the literature, content and discourse analysis, and a comparative examination of the digitalization strategies of the United States, China, the European Union, and Russia. The findings show that cyber conflict opens an enduring arena of contestation that complements rather than replaces traditional military force; that AI-enabled systems accelerate defense and intelligence processes while deepening problems of oversight and accountability; and that quantum computing is fundamentally altering the encryption order and approaches to national security. On the economic plane, the competition between central bank digital currencies and decentralized finance is redefining the notions of monetary sovereignty and financial control. The growing power of large technology companies calls state sovereignty into question, while disinformation and algorithmic targeting create new risks for democratic processes. The study concludes that digitalization is a multilayered process whose outcome is not predetermined, and that grasping this transformation requires extending the classical approaches to power and interdependence so as to encompass the command of data, algorithms, and networks.

Keywords: *Digitalization, Artificial Intelligence, Cybersecurity, Digital Sovereignty, Global Governance, International Relations*

DOI: 10.5281/zenodo.21320691

1. Introduction

The speed and pervasiveness that digital technologies have acquired over the past quarter-century have set in motion a transformation profound enough to unsettle the basic assumptions on which international relations rests. The ways in which states secure themselves, manage their economic resources, and negotiate with one another are being reshaped by developments in artificial intelligence, blockchain, quantum computing, and cybersecurity. The relationship between technological change and the structure of the international system is not a new question; yet the scope, speed, and borderless character of today's transformation set it apart from earlier industrial breakthroughs (Drezner, 2019). In the twenty-first century, a state's power is no longer measured solely by the number of its soldiers, its weapons capacity, or the size of its economy; it is also defined by its access to data, its ability to process that data, and its capacity to control critical digital infrastructure.

The concept of power itself has been reopened to debate in this process. Alongside the traditional understanding of power grounded in material resources, a new form of power has emerged that rests on the ability to steer information and to exert influence through networks (Nye, 2011). In a world of deepening interdependence, the channels that connect states to one another have at the same time become sources of vulnerability (Keohane & Nye, 2012). As Castells (2015) argued in his analysis of the network society, actors that hold the nodal points of information flows acquire a structural advantage along with the power to accelerate or sever those flows. Digitalization therefore does not merely supply new instruments; it also alters settled assumptions about the sources from which power springs and the ways in which it is exercised.

The domain in which this transformation is most visible is security. The forecasts of cyber conflict voiced in the years when the Cold War was ending (Arquilla & Ronfeldt, 1993) long remained a theoretical debate, but they turned into a concrete reality with events such as the 2007 attacks on Estonia and the Stuxnet malware that targeted Iran's nuclear facilities. Theorists are divided over whether cyber conflict can be considered war: one view holds that cyberattacks do not fully meet the criteria of lethality, destructiveness, and political purpose (Rid, 2013), while other work argues that this new "virtual weapon" constitutes a distinctive threat that transforms the international order (Kello, 2017). This new environment, in which states continuously surveil, sabotage, and destabilize one another, has blurred the line between espionage and attack (Buchanan, 2020; Segal, 2016). The emergence of cyber-conflict studies as a separate field of expertise in recent years likewise attests to the permanence of this phenomenon (Dunn Cavelty & Wenger, 2024).

Cyber threats have three core features that strain traditional theories of security. First, these threats transcend physical borders and render ineffective the protection once afforded by geographical distance. Second, because it is often impossible to determine the source of an attack with certainty, the problem of attribution weakens the very basis of deterrence. Third, states increasingly act through proxy actors, mercenary hackers, and private companies, which conceals responsibility and complicates the application of international law (Maurer, 2018). The balance-of-power and mutual-deterrence models developed during the era of nuclear deterrence lose their explanatory force in an environment where even the identity of the perpetrator remains uncertain (Buchanan, 2020).

Digital technologies have produced instruments that can be directed not only at infrastructures but also at social perception itself. Social media platforms, while enabling the rapid spread of information, have at the same time provided the ground for disinformation campaigns, manipulation, and polarization (Singer & Brooking, 2018). Interference in electoral processes, coordinated networks of fake accounts, and the production of synthetic content have given rise to a new form of conflict that targets public opinion. In this process, the algorithmic architecture of platforms quietly shapes the frame of political debate by deciding which content will be visible (Fuchs, 2021). The security threat has thus shifted from physical targets toward people's minds and decision-making processes.

The entry of artificial intelligence into defense and decision-making processes makes this picture still more complex. Autonomous systems, intelligence analysis, and rapid threat assessment are changing the way military and diplomatic decisions are made. The strategic use of artificial intelligence promises superiority on the one hand, while on the other it creates a source of power that is extremely difficult to govern, because the pace at which this technology develops far exceeds the speed at which the institutions meant to regulate it can adapt (Bremmer & Suleyman, 2023). The relationship between artificial intelligence and international relations theory is, moreover, a research field that has not yet matured; the extent to which existing theoretical tools can grasp the effects of this technology is open to debate (Ndzendze & Marwala, 2023; Arsenault & Kreps, 2024).

A less visible but potentially more disruptive development is taking place in the field of quantum computing. A quantum computer of sufficient capacity is expected to be able to break the encryption methods that today protect global communication and financial transactions. This expectation has already steered states and institutions toward the adoption of "quantum-resistant" encryption standards; indeed, the publication of post-quantum cryptography standards has been a concrete sign of this preparation (NIST, 2024a, 2024d). The consequences that quantum technologies carry for security and economic policy have entered the agenda of policy debate at the international level (OECD, 2025). The combined use of this technology with artificial intelligence, moreover, represents a threshold capable of simultaneously strengthening both defensive and offensive capabilities (Rodríguez, 2025).

Beyond security, the practice of diplomacy has also taken its share of this technological wave. The direct use of social media by foreign ministries and leaders as a tool of communication and influence has changed the form and pace of public diplomacy, giving rise to a new plane of interaction in which messages can reach broad audiences in an unmediated and instantaneous manner (Bjola & Holmes, 2015). The weight of soft power, defined as the capacity to obtain results through persuasion and attraction, has grown still greater in this environment (Nye, 2011). Yet the same channels also create the conditions for states to conduct influence operations targeting one another's publics, disrupting the traditional balance of diplomacy between openness and secrecy (Singer & Brooking, 2018). Digital tools thus widen states' repertoire of maneuver and bargaining while at the same time rendering crisis management more fragile (Segal, 2016).

DOI: 10.5281/zenodo.21320691

On the economic plane, digitalization is eroding the traditional instruments of control in states' hands. Data-driven business models, automation, and the platform economy have changed the structure of production and employment (Brynjolfsson & McAfee, 2014; Schwab, 2016). Blockchain technology carries the potential to transform payment and settlement processes by building systems that generate trust without a central authority (Kshetri, 2017); the tension between decentralized finance applications and central bank digital currencies is becoming a decisive debate over the future of the global financial architecture. The rapid growth of the digital economy is compelling states to redesign their instruments of taxation, regulation, and monetary policy (OECD, 2024). States are at the same time turning the advantage they hold in financial networks and their position in technology supply chains into instruments of pressure, thereby weaponizing economic interdependence (Farrell & Newman, 2023).

Perhaps the most contentious dimension of this transformation is the power acquired by non-state actors, and large technology companies in particular. The data, computing capacity, and infrastructural control concentrated in the hands of a few companies have turned these actors into players endowed with state-like authority (Zuboff, 2019). The roles that platforms assume in content moderation have acquired a quasi-sovereign function that determines the boundaries of public debate (Gorwa, 2019). States respond by extending their regulatory authority beyond their borders; the European Union's capacity to set standards on a global scale offers a clear example of this (Bradford, 2023). The embedding of the internet in every layer of everyday life has made the balance between control and freedom the central problem of governance (DeNardis, 2020); the concept of "digital sovereignty" has come to the fore as a framework invoked ever more frequently to name this tension, yet one whose content remains contested (Glasze et al., 2023).

A similar search for adaptation is under way on the legal and normative plane. How cyber operations are to be assessed within the existing framework of international law is being debated through the principles of sovereignty and non-intervention; efforts to resolve the uncertainties in this area have not yet reached a binding consensus (Schmitt, 2017; Moynihan, 2019). On the regulation of artificial intelligence, initiatives have accelerated at both the regional and the global level; the European Union's comprehensive regulation of artificial intelligence (European Parliament & Council, 2024), the principles and recommendations of international organizations (OECD, 2019), and the governance proposals developed within the United Nations (High-Level Advisory Body on Artificial Intelligence, 2024) are different manifestations of this effort. At the center of this regulatory search lie new concepts such as data sovereignty, algorithmic transparency, and the ethics of artificial intelligence, which are discussed as the new parameters of global governance (Roberts, 2024; Braun & Hummel, 2025). States' demand for control over data belonging to their own citizens and over the technologies they use also brings with it the question of for whose benefit and to what end digital sovereignty is being established (Mügge, 2024). The common feature of all these initiatives is that they can respond to the ethical and legal problems generated by technology only at a pace far behind the one that produces them (Floridi, 2018).

The fundamental problem revealed by this multilayered picture is that the literature seeking to explain the effects of digitalization on international relations remains, to a large extent, fragmented. Topics such as cybersecurity, the digital economy, artificial intelligence governance, and platform power are usually examined within separate fields of expertise, in isolation from one another. The criticism that the integration of the cyber domain with international relations theory has been delayed, and that these two fields have long ignored each other, is one indication of this disconnection (Foulon & Meibauer, 2024). Yet cyber politics, economics, and governance are interconnected parts of the same whole and can be analyzed meaningfully only within an integrated framework (Choucri, 2012). The rise of artificial intelligence has made still more visible the inadequacy of existing theories in grasping this technological transformation (Ndzendze & Marwala, 2023); calls for the systematic incorporation of technological change into international relations theory have grown stronger (Drezner, 2019).

Proceeding from this, the present study aims to analyze the effects of digital technologies on the international system in an integrated manner along the axes of security, economics, diplomacy, and law. By bringing together, within a common analytical framework, these areas that are mostly treated in isolation, the study seeks to assess the transformation that digitalization has brought about in international relations within a single theoretical narrative. The aim is thus not merely to describe the effects of individual technologies, but to show how these effects interact with one another and at which points they redefine the functioning of the international system.

The research is built around several core questions. First, it asks through which mechanisms digitalization alters the balance of power among states. Second, it considers to what extent cyber threats and AI-supported systems transform traditional understandings of security and deterrence. The third question concerns the effect of blockchain-based systems and digital currencies on states' instruments of economic control. Fourth, it examines how the power acquired by large technology companies redefines the concept of state sovereignty. Finally, it assesses the capacity of international law and normative frameworks to adapt to this rapid technological change.

The core propositions on which the research rests are that digitalization fundamentally alters the international balance of power, that cyber conflicts transform traditional security paradigms, and that digital financial systems erode states' economic sovereignty. These propositions offer a view oriented toward grasping the multidimensional effects of digital transformation as an interrelated whole. The study focuses in particular on the post-2000 period and on the digitalization strategies of principal actors such as the United States, the European Union, China, and Russia. This delimitation makes it possible to concentrate on the actors among whom digital power competition is most intense, while setting the scope of the analysis within a manageable frame.

Owing to the multidisciplinary and rapidly changing nature of the subject, the study adopts a qualitative research approach. Because the effects of digitalization, which cut across security, economics, and diplomacy at once, are too broad to be confined to a single method, an integrated design that combines theoretical analysis with comparative assessment has been preferred. In the theoretical analysis, the network approach is drawn upon to grasp the distribution of digital power across networks, while technological determinism, constructivism, and critical perspectives are used to assess the relationship of technology with social structures. The

DOI: 10.5281/zenodo.21320691

analysis rests largely on academic literature, states' strategy documents, the reports of international organizations, and the statements of technology companies. While these sources offer a rich picture, the limited availability of publicly accessible data in areas such as cyber operations, intelligence activities, and secret strategic plans constitutes a natural constraint on empirical analysis. This constraint is openly acknowledged, and the findings are interpreted within this frame.

Within this framework, the original contribution of the research is that it brings together, on a common theoretical ground, technological domains that are mostly examined separately, and that it treats digitalization not as an isolated technical innovation but as a political, economic, and social phenomenon that transforms the fundamental dynamics of the international system. The findings of the study are expected both to contribute to academic debate in the direction of updating the discipline's theoretical tools and to serve as a guide for policymakers seeking to manage technological transformation. The subsequent sections of the article carry out this aim step by step, respectively through the assessment of the relevant literature, the construction of the theoretical framework, the explanation of the method followed, and the presentation and discussion of the findings.

2. Literature Review

The body of scholarship addressing the impact of digital technologies on international relations has expanded rapidly over the past two decades; yet this growth has occurred not around an integrated theory but in the form of research clusters that are largely unaware of one another. The classical heritage of the discipline explains power mostly in terms of material resources, that is, military capacity, population, and economic size. Keohane and Nye's analysis of interdependence gave this approach an early flexibility, showing that states are bound to one another not only by weapons but also through channels of communication and institutions, and that these bonds produce asymmetric power relations in the form of sensitivity and vulnerability (Keohane & Nye, 2012). Nye's emphasis on the soft and smart components of power in the information age, together with his observation that power is diffusing toward non-state actors, is another important way station along the same line (Nye, 2011). Drezner, by contrast, argues that technological change long remained a secondary variable in international relations theory, often treated as an exogenous given rather than woven into the theory itself (Drezner, 2019). Choucri, for her part, produced one of the first comprehensive attempts to define cyber politics as a distinct object of research by placing the cyber domain directly at the center of analysis (Choucri, 2012).

The network-society literature emphasizes that power is increasingly built through control over information flows. Castells shows, with concrete examples, the capacity of digital networks to mobilize social movements and shape the political agenda, demonstrating how horizontal organization strains traditional structures of power (Castells, 2015). DeNardis argues that in the age of the internet of things, infrastructure itself becomes a question of security and freedom, and that internet governance is now not merely a technical but a deeply political matter (DeNardis, 2020). At the same time, strong claims that digitalization is rebuilding the international system entirely from scratch have recently met with cautious criticism. Foulon and Meibauer take a measured position against the language of revolution, arguing that the cyber domain does not change the structure of international relations but rather affects mechanisms such as deterrence, the choice of foreign policy tools, and uncertainty as a "structural modifier" (Foulon & Meibauer, 2024). Ndzendze and Marwala likewise show that new technologies are not an entirely extra-theoretical domain by rereading artificial intelligence in the language of established theories such as realism, liberalism, and constructivism (Ndzendze & Marwala, 2023).

The oldest and still unsettled debate in the security literature concerns the nature of the cyber threat. As early as the 1990s, Arquilla and Ronfeldt heralded the coming of cyberwar, foreseeing that conflict in the information age would be networked and information-centric (Arquilla & Ronfeldt, 1993). Rid directly opposes this framing; for him, what has occurred to date is not war in any genuine sense but sabotage, espionage, and disruptive effect, because cyber acts do not meet the criteria of lethality, instrumentality, and political character all at once (Rid, 2013). Standing between these two poles, Kello defines cyber conflict as an intermediate condition that is neither full peace nor full war and draws attention to its destabilizing effect on the international order (Kello, 2017). Segal reads the post-2012 period as a "hacked world order" in which states openly contend with one another (Segal, 2016). Buchanan, in turn, shows that state-sponsored operations are largely covert and continuous and operate very differently from catastrophic scenarios, following instead a logic of "signaling and shaping" through espionage, sabotage, and destabilization (Buchanan, 2020). Maurer, examining the relationships states establish with proxy hacker groups, describes a regime of delegation and orchestration in which responsibility is deliberately blurred (Maurer, 2018). Dunn Cavelty and Wenger, mapping the evolution of the field, show that cyber-conflict research has moved from its early prophetic tone toward an empirically and theoretically more cautious stage (Dunn Cavelty & Wenger, 2024).

Alongside the theoretical debate, the threat reports published regularly in recent years have given this literature an empirical footing. Microsoft's annual digital defense reports document the numerical increase in espionage and influence operations by state-linked actors and the blurring of the boundary between these actors and financially motivated crime networks (Microsoft, 2024, 2025). The threat-landscape reports of the European Union Agency for Cybersecurity show that ransomware and supply-chain attacks have become a persistent risk for critical infrastructure (European Union Agency for Cybersecurity [ENISA], 2024, 2025). The World Economic Forum, for its part, emphasizes that cyber risks are distributed unevenly, are intertwined with geopolitical tension, and that the resilience gap between large organizations and small actors is widening (World Economic Forum [WEF], 2025, 2026). These reports document a point the academic literature often overlooks: the cyber threat operates less through individual destructive attacks than as a low-intensity but continuous form of pressure.

The legal status of cyber operations is a separate and as yet unresolved area of debate. The Tallinn Manual 2.0 proposes a common legal language for the field by elaborating, through the principles of sovereignty, non-intervention, and the use of force, how existing international law applies to cyber operations; yet this text is not a binding treaty but a compilation of expert opinion and does not reflect full consensus among states (Schmitt, 2017). Moynihan, examining the uncertainties in assessing state-originated cyberattacks in terms of the principles of sovereignty

DOI: 10.5281/zenodo.21320691

and non-intervention, shows how the problem of attribution in particular weakens legal responsibility (Moynihan, 2019). The difficulty of proving which actor an attack belongs to directly hampers both deterrence and the operation of the principle of proportionate response.

The impact of artificial intelligence on international relations is the fastest-growing but also the most divided branch of the literature. Agrawal, Gans, and Goldfarb treat artificial intelligence as a "prediction machine" and argue that the real transformation lies not in individual products but in the way cheaper prediction reorganizes all decision-making processes, that is, at the system level (Agrawal et al., 2022). Acemoglu and Johnson, for their part, show that the direction of technology is not natural but a political choice; that automation does not by itself produce shared prosperity; and that the distribution of gains and losses depends on institutional power relations (Acemoglu & Johnson, 2023). Bremmer and Suleyman argue that artificial intelligence creates a power paradox that seats states and technology companies at the same table, and that companies have entered the geopolitical equation as a type of actor not bound to geography (Bremmer & Suleyman, 2023). Arsenault and Kreps define artificial intelligence as an "enabling power" that multiplies states' capabilities (Arsenault & Kreps, 2024). Srivastava and Bullock, for their part, show that digital sovereignty is interwoven between public and private power by tying the instrumental, structural, and discursive forms of power that artificial intelligence affords states and companies to the domains of violence, the market, and rights (Srivastava & Bullock, 2024). West focuses on the labor-market dimension of the transformation, addressing the effects of automation on employment and inequality (West, 2018), while Crawford analyzes artificial intelligence not as an abstract mass of code but as a material apparatus that rests on natural resources, human labor, and data, and that concentrates power in a few centers (Crawford, 2021).

On the regulatory side, too, there is a rapidly expanding institutional literature. The Organisation for Economic Co-operation and Development's recommendation on artificial intelligence set out the first intergovernmental set of common principles, establishing criteria for trustworthy artificial intelligence (Organisation for Economic Co-operation and Development [OECD], 2019). The European Commission's white paper drew the framework of a risk-based approach built on the duality of excellence and trust (European Commission, 2020); this line acquired legal form with the Artificial Intelligence Act, the first comprehensive and binding legislation on artificial intelligence (European Parliament & Council of the European Union, 2024). On the side of the United States, a voluntary and flexible risk-management framework has been preferred (National Institute of Standards and Technology [NIST], 2023). At the global level, the United Nations' High-Level Advisory Body on Artificial Intelligence proposes an inclusive global framework by identifying the gaps in existing governance mechanisms (High-Level Advisory Body on Artificial Intelligence, 2024), while the United Nations' Our Common Agenda report has prepared the ground for initiatives such as the Global Digital Compact (United Nations, 2021). Stanford's AI index, for its part, shows with data that investment, model capacity, and the talent pool are concentrated in particular countries, revealing the concrete dimensions of the asymmetry in this field (Stanford Institute for Human-Centered Artificial Intelligence, 2024).

The theoretical core of these regulatory debates is the concept of digital sovereignty. Bradford reads the global digital order through three regulatory empires: the market-driven American model, the state-driven Chinese model, and the rights-driven European model; these models spread in a competition that is both vertical, through companies, and horizontal, among states (Bradford, 2023). O'Hara and Hall set out a similar distinction through the metaphor of "four internets," showing that Silicon Valley's open, Brussels's rights-based, Washington's commercial, and Beijing's state-controlled conceptions of the internet are diverging from one another and that this heightens the risk of internet fragmentation (the splinternet) (O'Hara & Hall, 2021). The concept itself is not free of criticism. Braun and Hummel question the normative grounds of the concept by arguing that the discourse of digital sovereignty often rests on a one-dimensional and overly simplified understanding of sovereignty (Braun & Hummel, 2025). Glasze and colleagues examine the spatial and geopolitical dimensions of digital sovereignty, discussing how the concept is rearticulated with geography (Glasze et al., 2023). Mügge draws attention to the dimension of class and interest in the concept by questioning for whom, to what end, and to whose benefit Europe's discourse of AI sovereignty operates (Mügge, 2024); Roberts, in turn, seeks to place the issue within a normative framework in the context of artificial intelligence (Roberts, 2024).

Along the axis of economic policy, the literature emphasizes that digital infrastructures do not merely facilitate trade but have also become an instrument of coercion. Farrell and Newman show that the concentration in the hands of a few states of chokepoints such as financial messaging networks, dollar clearing, and semiconductor supply chains turns interdependence into a weapon (Farrell & Newman, 2023). Brynjolfsson and McAfee analyze the dual effect of digital technologies, which increase productivity while deepening inequality, through the concept of the "second machine age" (Brynjolfsson & McAfee, 2014); Schwab, for his part, names the convergence of technologies the fourth industrial revolution (Schwab, 2016). In the blockchain debate, Kshetri assesses in a measured way that this technology carries both opportunity and risk in terms of security and privacy (Kshetri, 2017); the OECD digital economy outlook, for its part, sets out with data the concentration of digital markets and cross-border data flows (OECD, 2024). The most current extension of this line is the tension between central bank digital currencies and decentralized finance applications; this rapidly growing debate, in terms of monetary sovereignty, control over payment infrastructures, and the effectiveness of sanctions, remains in the literature largely at a descriptive level and appears to lack a settled theoretical framework. Ding, for his part, brings an important corrective to this entire literature: for him, what determines power transitions is not in whom a technology is first invented but the extent to which that technology can diffuse across the whole economy; the real arena of competition is therefore not patents but the institutional capacity that makes diffusion possible (Ding, 2024).

Quantum technologies, as one of the most decisive future thresholds of security, are also rapidly gaining a place in the literature. The post-quantum cryptography standards published by the American standards institute aim to produce a response to the vulnerability of existing encryption to quantum computers by formalizing lattice-based key-encapsulation and digital-signature methods and a stateless hash-based signature scheme (NIST, 2024a, 2024b, 2024c); the transition to these standards has been planned through a separate roadmap (NIST, 2024d). The urgency

DOI: 10.5281/zenodo.21320691

of standardization stems from the threat, termed "harvest now, decrypt later," that encrypted data captured today could be decrypted in the future with quantum capacity. The OECD's policy primer on quantum technologies emphasizes that this transition is not merely technical but at the same time a matter of policy and investment (OECD, 2025). Rodríguez, for his part, examines how quantum computing, when used together with artificial intelligence, could transform both offensive and defensive capabilities, pointing in particular to the importance of investment in quantum networks for defense (Rodríguez, 2025).

The rise of non-state actors constitutes another dense vein of the literature. Zuboff argues that large technology companies have built a surveillance capitalism that operates through the "behavioral surplus" derived from user behavior and that commodifies human experience, giving rise to a new instrumentarian form of power (Zuboff, 2019). Gorwa defines the concept of platform governance and analyzes how the authority to moderate content and to set rules is shared between states and private platforms (Gorwa, 2019); Fuchs, for his part, addresses social media from the perspective of critical political economy, rendering visible the relations of data, labor, and capital (Fuchs, 2021). Floridi names digitalization the "fourth revolution" and draws a picture of an infosphere in which the human being repositions itself as one among informational entities (Floridi, 2014), arguing that this transformation should be governed by a "soft ethics" beyond binding law (Floridi, 2018). Taken together, these works point to a consensus on the claim that technology companies have become not merely economic actors but quasi-public centers of power that shape global norms.

One of the most visible forms of the digital threat is the use of information itself as a weapon. Singer and Brooking, showing with a broad repertoire of examples that social media has turned into an arena of conflict and that viral content, automated accounts, and organized manipulation have become an inseparable part of political struggle, name this phenomenon "LikeWar" (Singer & Brooking, 2018). This approach treats disinformation not as a marginal side effect but as a systematic strategy aimed at shaping public opinion. That the capacity for horizontal mobilization described by Castells (Castells, 2015) can be operated in reverse with the same tools—that is, used to deepen social polarization and to interfere in electoral processes—reveals the two-sided nature of digital networks. One end of the problem connects directly to platform governance: the uncertainty over by what standard and by whom content will be moderated creates an unresolved conflict of authority between states and private platforms (Gorwa, 2019). The tension between Europe's search for rights-based regulation and the data-collection logic of surveillance capitalism becomes evident precisely at this point. Moreover, the fact that generative artificial intelligence is making the production of fake text, audio, and imagery cheaper signals that this threat will grow heavier still in the near future (WEF, 2025, 2026).

Assessed as a whole, this body of work reveals two basic limitations. First, the field is largely siloed: the cyber-conflict literature, the AI-governance literature, the digital-sovereignty debate, the political economy of financial chokepoints, quantum-security research, and studies of information warfare and platform power often advance unaware of one another, and a framework that integrates the points at which these technologies intersect and reinforce one another remains absent. Second, the discipline's delay in internalizing technology leads the impact of digitalization on the international system to be read in binary terms, as either a revolutionary rupture or a simple continuity; whereas more nuanced studies show that the impact varies by domain and mechanism (Foulon & Meibauer, 2024; Dunn Cavelty & Wenger, 2024). Drezner's warning about the gap in the theorization of technological change also remains largely valid (Drezner, 2019). It is precisely here that this article aims to remedy both gaps at once, by proposing an integrated analytical framework that connects the aforementioned research clusters along the axes of security, economics, diplomacy, and law.

3. Theoretical Framework and Analytical Approach

It is difficult to explain the impact of digital technologies on international relations through a single theory, because that impact bears at once on the distribution of power, the structure of actors, norms, and institutions. The analysis here is therefore built upon three complementary theoretical strands. The first is the network-based approach, which shows how states and non-state actors gain power through connections. The second is the triad of technological determinism, constructivism, and critical theory, which read the social and political consequences of technology through different assumptions. The third is a technology-focused assessment that addresses at which points pioneering technologies such as artificial intelligence, blockchain, and quantum strain established theories. When these three strands are brought together, it becomes clear that digitalization does not merely supply new instruments but also changes the operating logic of the international system (Drezner, 2019; Choucri, 2012).

Traditional analyses mostly treat international relations as a vertical order among states. The network approach, by contrast, places at its center how actors are connected to one another and how these connections distribute power. Castells's concept of the network society describes how the vertical organization of the industrial age has given way to flexible structures in which information circulates horizontally among nodes (Castells, 2015). In this reading, an actor's weight is determined not only by the material resources it holds but by its position within the network—that is, by how many nodes it is connected to and through which points the flow is compelled to pass. Keohane and Nye's analysis of multichannel interdependence heralded this logic early on: the more channels through which actors are connected to one another, the more the severability of these connections becomes a political resource (Keohane & Nye, 2012).

The weaponization of interdependence is one of network theory's most concrete contributions to the digital age. Farrell and Newman show that global finance, communication, and data networks operate through certain passage points; that the state controlling these points can gather information about everyone connected to the network and, when necessary, expel actors from it (Farrell & Newman, 2023). The paralysis of a country's foreign trade once it is removed from the SWIFT payment system, or the cutting of access to particular semiconductor supply chains, are current examples of this chokepoint power. As DeNardis emphasizes, the invisible infrastructure of the internet—that is, naming systems, routing protocols, and certificate authorities—establishes a similar layer of control; decisions that appear technical often produce political consequences (DeNardis, 2020). Digital power thus comes to be a matter less of the capacity one possesses than of holding the points through which the flow passes.

DOI: 10.5281/zenodo.21320691

In an order where networks distribute power, information itself is a strategic resource. Digitalization has removed the ability to produce and disseminate information from the monopoly of states, making platform companies, organizations, and ordinary users part of this process as well. But the same openness also opens the door to manipulation. Singer and Brooking describe how social media has turned virtually into a battlefield; how, through algorithmic spread, micro-targeting, and networks of automated accounts, content tailored to a narrow audience can reach millions in a short time; the online influence campaigns directed at the 2016 US presidential election are the most studied example of this, and they show that borders can no longer stop such operations and that a country's public opinion can be shaped from outside (Singer & Brooking, 2018). Zuboff's analysis of surveillance capitalism, for its part, shows the commercial face of the matter: the data derived from user behavior produces both profit and the power to predict and steer behavior in advance (Zuboff, 2019).

The fact that the greater part of information flows is controlled by a few technology companies (GAFAM, for short) has removed the digital balance of power from being in states' favor. Because these companies hold basic layers such as search, social networking, the cloud, and mobile operating systems, they have turned into infrastructure providers on which even states are dependent. Bradford says that this picture has given rise to a competition among three distinct regulatory models: the American model that privileges the market, the European model that privileges rights, and the Chinese model that privileges the state (Bradford, 2023). Gorwa's discussion of platform governance shows that by whom and according to what criteria content is to be moderated has itself turned into a problem of sovereignty (Gorwa, 2019). All of this has brought to the agenda states' search for control over the data and infrastructure within their own borders—that is, the concept of digital sovereignty (Glasze et al., 2023).

The search for digital sovereignty carries a paradox. As sates seek to strengthen their autonomy through data localization, national technology champions, and the reduction of external dependence in critical areas, they also heighten the risk of fragmenting the global network. The European Union's effort to turn privacy into a worldwide criterion through the General Data Protection Regulation, and China's effort to legitimize a network closed within its borders through the doctrine of cyber sovereignty, represent two opposing value systems loaded onto the same technology (Bradford, 2023; Glasze et al., 2023). This situation is often referred to as the splinternet, in the sense of the formation of disconnected digital zones in place of a single global internet. The question of whose values the norms will be written according to is a dimension as decisive in the struggle for digital power as material capacities are (Drezner, 2019).

Beneath this analysis of power lie three distinct theoretical stances on the relationship of technology with society, and each reads the same phenomena differently. The first, technological determinism, sees technology as an independent force advancing through its own internal logic, and social and political structures as elements obliged to adapt to it. The classic debate compiled by Smith and Marx sets out both the appeal and the limit of this approach: the intuition that technology drives history is strong, but this intuition renders invisible the social choices that determine in which direction technology develops (Smith & Marx, 1994). Brynjolfsson and McAfee's analysis of the second machine age and Schwab's concept of the fourth industrial revolution largely narrate digital transformation in this language of inevitability (Brynjolfsson & McAfee, 2014; Schwab, 2016). Floridi's reading of the information revolution likewise speaks of a threshold that radically changes the human being's understanding of itself and the world (Floridi, 2014). The contribution of the determinist view is that it takes seriously the speed and pervasiveness of digitalization; its shortcoming is that it overlooks the fact that technology is shaped within particular interests and values.

The second stance, constructivism, begins precisely where determinism falls short. The social theory developed by Wendt argues that the behavior of actors in the international system is determined not only by material capacities but by shared meanings, identities, and mutual expectations (Wendt, 1999). In this reading, a technology does not by itself impose an outcome; the meaning loaded onto it produces the outcome. While one state counts the same blockchain system as an instrument of economic independence, another may see it as a threat to the financial order. China's Digital Silk Road initiative, too, is not merely an infrastructure investment but at the same time the construction of an identity of global leadership. Finnemore and Sikkink's model of the norm life cycle offers a suitable framework for tracking how new norms, such as appropriate behavior in the cyber domain, emerge, spread, and become internalized (Finnemore & Sikkink, 1998). As Checkel reminds us, the real strength of constructivism lies in showing identity and interest not as fixed givens but as variables constructed in interaction (Checkel, 1998).

The third stance, critical theory, reads digitalization within existing power relations and capital accumulation, and foregrounds the question of for whose benefit. Zuboff names a regime of accumulation in which user behavior is turned into data and data into prediction products surveillance capitalism (Zuboff, 2019). Fuchs analyzes social media as a relation of exploitation built on advertising and data (Fuchs, 2021). Couldry and Mejias go further still, conceptualizing as data colonialism this process in which every moment of human life is appropriated as raw data; they say that the appropriation of land and body by historical colonialism has today been replaced by the appropriation of life itself (Couldry & Mejias, 2019). This analysis also renders visible the material leg of the digital—that is, the energy of data centers, the raw materials of hardware, and the labor of labeling—thereby exposing the inequalities concealed by the discourse of technological progress. Acemoglu and Johnson likewise emphasize that technology does not by its nature spread prosperity, and that to whom the gain will go is a matter of choice and power (Acemoglu & Johnson, 2023).

Another focus of the critical view is that digital tools are as suitable for control as they are for emancipation. In the early period, the expectation that the internet would be democratizing was widespread. Morozov, however, showed that the same technologies can be used at least as effectively by authoritarian governments for surveillance, censorship, and monitoring of the opposition (Morozov, 2011). AI-supported facial recognition, content filtering, and behavior-scoring systems have today carried this capacity for control much further. The fact that the same technology turns in one place into a rights framework that protects privacy and in another into an apparatus of control that continuously monitors the citizen shows that the outcome is hidden not in the technology itself but in the institutional and normative order that surrounds it. The political consequence of digital technology is therefore not given in advance; it depends on the framework within which it is used.

DOI: 10.5281/zenodo.21320691

These three theoretical stances work together in analyzing the problems that pioneering technologies create in international relations. Foremost among these is artificial intelligence, which carries power competition beyond military and economic capacities. Ndzendze and Marwala argue that artificial intelligence is for international relations theories not merely a new topic but a domain that tests the theories themselves; that the machine-supported character of decision-making, prediction, and alliance calculations requires rethinking the discipline's basic assumptions (Ndzendze & Marwala, 2023). Arsenault and Kreps draw attention to artificial intelligence becoming both an instrument and a subject of foreign policy (Arsenault & Kreps, 2024). Agrawal, Gans, and Goldfarb's analysis, for its part, shows that artificial intelligence is in essence a technology that produces cheap prediction and that precisely for this reason it shifts strategic balances by changing the costs of decision-making (Agrawal et al., 2022).

The applications of artificial intelligence in the field of security are the heading that most strains classical theories. Autonomous weapon systems, machine-supported intelligence analysis, and accelerated command loops reopen for debate such established concepts as deterrence and the security dilemma. The delegation of decisions to the machine heightens the risk that escalation in crises will slip beyond human control; the inability to determine the source of an attack with certainty—that is, the problem of attribution—renders deterrence based on retaliation uncertain (Kello, 2017). The tension between the expectation of cyberwar that Arquilla and Ronfeldt heralded as early as the 1990s and Rid's criticism, which finds this concept exaggerated and argues that the real threat is espionage, sabotage, and destruction, constitutes the still-live questions of the field (Arquilla & Ronfeldt, 1993; Rid, 2013). The relationship states establish with proxy hacker groups, examined by Maurer, likewise creates a gray zone in which responsibility is deliberately blurred (Maurer, 2018).

The entry of artificial intelligence into diplomacy and governance brings speed and efficiency while also enlarging the problem of accountability. Bremmer and Suleyman name the gap between the speed at which technology develops and the speed at which the institutions meant to govern it develop a power paradox: states can regulate this technology in a timely manner neither on their own nor through existing organizations (Bremmer & Suleyman, 2023). Initiatives aimed at closing this gap have rapidly multiplied. The European Union first drew a roadmap in this field with the 2020 white paper (European Commission, 2020) and then put into force the risk-based and binding Artificial Intelligence Act (European Parliament & Council of the European Union, 2024). By contrast, America's voluntary risk-management framework (National Institute of Standards and Technology [NIST], 2023), the OECD's non-binding principles (Organisation for Economic Co-operation and Development [OECD], 2019), and the United Nations' proposal for governance on a global scale (High-Level Advisory Body on Artificial Intelligence, 2024; United Nations, 2021) offer alternatives at varying degrees of stringency. Floridi's concept of soft ethics comes to the fore, alongside these hard regulations, as a complementary framework that guides responsible conduct in areas the law has not yet caught up with (Floridi, 2018). The multiplicity of these frameworks shows that a single global standard has not yet formed. Measurements showing that AI capabilities have rapidly concentrated in recent years suggest that the gap between regulation and technology may widen still further (Stanford Institute for Human-Centered Artificial Intelligence, 2024). The effect of these technologies on the labor force and social structure is likewise an inseparable part of the debate (West, 2018).

The second pioneering technology, blockchain, with its promise of secure and immutable record-keeping without the need for a central authority, calls into question the state's traditional instruments of control. Kshetri examines the protection this architecture provides in terms of data integrity and privacy as well as the new vulnerabilities it brings (Kshetri, 2017). The technology's real effect in international relations is seen in the monetary domain. The tension between central bank digital currencies and decentralized finance reflects the conflict between the state's monopoly over money and the promise of disintermediated transactions. China's digital yuan and the European Union's work on a digital euro show the different strategies of states for bringing this technology under control. Here, too, Farrell and Newman's chokepoint logic is decisive: holding the payment infrastructure is directly connected to the power to impose sanctions, while decentralized systems carry the potential to erode this power (Farrell & Newman, 2023). As the constructivist reading reminds us, whether the same technology is counted as an instrument of independence or a threat to order remains tied to the meaning loaded onto it.

The third and perhaps most disruptive technology, quantum computing, threatens the foundation of today's encryption order. Quantum computers that draw on the principles of superposition and entanglement have the capacity to break, in theory, widely used public-key encryption methods (Organisation for Economic Co-operation and Development [OECD], 2025). The most insidious aspect of this is that encrypted data captured today can be stored to be broken in the future—that is, the "harvest now, decrypt later" threat—which turns security into a problem carried from today into the future. Rodríguez shows that the combination of quantum with artificial intelligence enlarges the threat still further (Rodríguez, 2025). In response to the risk, post-quantum encryption standards have been developed; the algorithms and transition roadmap published by the American standards body are concrete steps of this preparation (National Institute of Standards and Technology [NIST], 2024a, 2024b, 2024c, 2024d). The threat that quantum carries for nuclear command-and-control and strategic communication systems requires a reexamination of the theories of deterrence and strategic stability; the technology's dual-use nature—open to both civilian and military use—makes it difficult to establish a control regime akin to disarmament (Choucri, 2012).

None of these technologies operates independently of law and norms. How state-originated cyberattacks are to be assessed in terms of the principles of sovereignty and non-intervention is still contested (Moynihan, 2019). The Tallinn Manual 2.0, prepared by experts, is the most comprehensive effort regarding how existing international law might apply to cyber operations, but it is not a binding treaty (Schmitt, 2017). Cyber-conflict studies are themselves in a process of theoretical maturation (Dunn Cavelty & Wenger, 2024); analyses arguing that cyberspace transforms international relations through structural modifiers are current products of this maturation (Foulon & Meibauer, 2024). Segal's analysis of statecraft in the digital age shows how all these dimensions are interwoven within a single hacked world order (Segal, 2016). The concrete ground of the theoretical debate, for its part, is constituted by the empirical data in industry and institutional reports: measurements showing that the threat

DOI: 10.5281/zenodo.21320691

environment grows heavier each year remove the analysis from being an abstract exercise in theory (Microsoft, 2025; European Union Agency for Cybersecurity [ENISA], 2025; World Economic Forum, 2026).

Finally, all these strands intersect in the normative dimension of digital sovereignty. Whether carrying sovereignty into the digital domain is desirable is contested. Mügge questions whose interest Europe's discourse of AI sovereignty serves (Mügge, 2024); Roberts proposes a normative framework to render digital sovereignty defensible (Roberts, 2024); Braun and Hummel, for their part, object to the often unquestioning affirmation of the concept (Braun & Hummel, 2025). Srivastava and Bullock set out the necessity of reading artificial intelligence, global governance, and digital sovereignty together (Srivastava & Bullock, 2024). Assessed all together, it is clear that grasping digitalization through a single theory will fall short. The network approach shows where power accumulates, the three meta-theories show by what logic this accumulation is to be read, and the technology-focused analysis shows which new problems arise. The following sections test this integrated framework through concrete developments in the fields of security, economics, diplomacy, and law.

4. Research Method

The aim of this section is to set out clearly which questions the study answers, with what research design, and on what grounds. The research is built around three core questions: How do digital technologies redefine states' power capacities and their understanding of sovereignty? Through what pathways do technologies such as artificial intelligence, cyber capabilities, quantum computing, and blockchain transform international competition in the fields of security, economics, and diplomacy? In the face of this transformation, to what extent can traditional theories of international relations remain explanatory? These questions require understanding the "how" and "why" dimensions of a current phenomenon within its own real context; such questions are answered not through quantitative measurement but through case-based qualitative designs and an analytical rather than statistical conception of generalization—that is, by carrying the findings not from a sample to a population but from empirical material to theoretical propositions (Yin, 2018). The study therefore rests on an interpretive, qualitative, and theory-building design. The unit of analysis is not individual technologies but the field of digital power that grasps a state's digital strategy as a whole; the temporal focus, for its part, is the period extending from the decisive debates over digital interference in 2016 to the present.

Behind this design lies a particular conception of knowledge. The phenomenon under examination is still in flux; it is a field in which numerous causes are interwoven and which cannot be tested under controlled conditions by isolating variables from one another. The interpretive paradigm assumes that social reality is constituted through the meanings that actors load onto it; the researcher's task, in turn, is to read these meanings within their context (Creswell & Poth, 2018). Because the subject extends from security to economics and from diplomacy to law, it would be misleading to confine oneself to a single discipline. An interdisciplinary perspective has therefore been adopted, drawing not only on international relations but also on the literatures of computer science, law, economics, and sociology.

The analysis is theoretically guided. Realism, liberalism, and constructivism, together with the debate over technological determinism, have been used as lenses that determine what matters when looking at the field. The realist lens serves to focus on states' pursuit of power and security, the liberal lens on interdependence and cooperation, and the constructivist lens on the construction of norms, identities, and discourses. To avoid the blind spots that reliance on a single theory would produce, these lenses have been deliberately held together. The inference has thus been neither purely inductive nor purely deductive; an abductive reasoning has been followed that moves back and forth between theory and data, working together the categories derived from theory with the patterns emerging from the texts.

The cases were selected not at random but purposively, since the aim in qualitative research is not statistical representation but reaching examples that can illuminate the subject in the richest way (Patton, 2015). With this logic, the United States, China, Russia, and the European Union have been identified as the principal cases. These four actors differ markedly from one another in terms of political regime, strategic culture, and technological capacity. This difference among them has been deliberately sought, because it renders visible how regime type and strategic tradition shape digital policies. This approach, which by placing side by side examples as different from one another as possible reveals both common patterns and points of divergence, rests on a well-established tradition of comparative case study (George & Bennett, 2005; Gerring, 2007). China's New Generation Artificial Intelligence Development Plan and Digital Silk Road initiative, the United States' national artificial intelligence and cybersecurity strategies, Russia's digital influence operations targeting electoral processes, and the European Union's value-based regulatory model constitute the concrete material of this comparison. This selection also brings with it a deliberate limit: the framework has been narrowed to great-power competition, and the experiences of the Global South have not been addressed directly as cases; this choice has been made in order to preserve the focus of the comparison and has been kept in view in the interpretation of the results.

The study's database is two-layered. Its primary layer consists of the official texts produced by the actors themselves: national security documents, artificial intelligence and cybersecurity strategies, defense doctrines, and legal regulations. Its secondary layer, in turn, is made up of peer-reviewed academic publications, the reports of international organizations, think-tank analyses, and industry reports. The United Nations' high-level advisory report on AI governance (High-Level Advisory Body on Artificial Intelligence, 2024), the European Union Agency for Cybersecurity's threat-landscape assessment (European Union Agency for Cybersecurity, 2024), the World Economic Forum's cybersecurity outlook (World Economic Forum, 2025), and, from the private sector, Microsoft's annual digital defense report (Microsoft, 2025) are typical examples of this layer. Official documents are not neutral by themselves; they are social products created for a particular purpose, to address a particular audience, and must therefore be read with a critical eye, taking into account the context in which they were produced (Bowen, 2009). Accordingly, the criteria of reliability, currency, and relevance were observed in source selection; and so that the perspective of a single geography or institution would not dominate the analysis, literature originating from the West, China, and Russia was surveyed in a balanced way.

The data were processed through a four-stage analytical strategy. In the first stage, the method of structured, focused comparison

DOI: 10.5281/zenodo.21320691

was applied; this method requires posing predetermined common questions to each case and thereby disciplines the comparison across cases (George & Bennett, 2005). States' technological capacity, regulatory choices, security discourses, and governance vision were addressed around these common questions, so that a systematic comparison was obtained rather than scattered observations.

In the second stage, qualitative content analysis was carried out. Content analysis treats texts not as merely physical data but as messages that carry meaning within the social context in which they are produced and read (Krippendorff, 2018). Coding was conducted both with categories derived from theory and with categories arising from the texts themselves; in the literature these are termed directed and conventional content analysis, respectively (Hsieh & Shannon, 2005). While predefined codes such as power, sovereignty, security, and cooperation were tracked in the documents, the list of codes was expanded as unexpected themes emerged. To preserve consistency among the codes, the principle of constant comparison was adopted; each new document was coded by being compared with the categories previously established, and the categories were rearranged as needed. The emphasis was placed less on counting words than on making sense of the implicit priorities, value orientations, and lines of tension in the documents.

In the third stage, discourse analysis came into play. The assumption that language not only describes reality but also constitutes it and is interwoven with relations of power is the point of departure of this method (Fairclough, 2013). In particular, the securitization approach, which explains how an issue, when narrated in the language of an "existential threat," is carried beyond ordinary politics and drawn into the field of security, offers a suitable ground for reading whether digital issues are framed as a threat or an opportunity (Buzan et al., 1998). Accordingly, the distinction between the emphasis on "cyber sovereignty" by Chinese and Russian officials and the United States' discourse of an "open internet" has been analyzed not as a mere difference of style but as the expression of separate conceptions of the world. The tradition of discourse analysis in the international relations literature has been a guide in the intertextual and context-sensitive examination of security discourses (Hansen, 2006).

In the fourth stage, network analysis was used. Digital governance is no longer a field in which only states are on stage; international organizations, technology companies, and civil society organizations are also influential actors in this field. Network analysis, by rendering visible the patterns of relations among actors, makes it possible to redefine power through positional concepts such as access, brokerage, and exclusion, thereby offering a notable contribution to the classical understanding of power in international relations (Hafner-Burton et al., 2009). Concepts such as centrality and brokerage are drawn from the established toolkit of social network analysis (Wasserman & Faust, 1994). In this study, these concepts have been employed less for quantitative measurement than for relational mapping, in order to describe the multilayered structure of digital governance and the concentrations of influence within it.

The combined use of these four methods is not incidental. Operating together different data sources, different methods, and different theoretical lenses reduces the distortions that reliance on a single source or technique would produce; in the literature this is known as data, method, and theory triangulation, respectively (Denzin, 1978; Flick, 2018). What one method overlooks is expected to be caught by another, and when the findings point in the same direction, the interpretation is expected to rest on a firmer footing.

In a qualitative study, reliability and validity do not coincide exactly with the criteria of experimental research; in their place, the criteria of credibility, transferability, dependability, and confirmability are taken as the basis (Lincoln & Guba, 1985). Credibility expresses the consistency of the analysis with the data and has been strengthened by examining the sources over a long period, again and again. Transferability requires that the context be described in sufficient detail for the findings to be carried into other contexts; the cases have therefore been addressed with thick rather than superficial description. Dependability concerns whether the steps followed can be traced by others; the process extending from source selection to coding has therefore been documented, through a codebook and decision records, in a way that leaves an auditable trail. Confirmability, in turn, aims to show that the interpretations derive from the data rather than from the researcher's biases. To tie these criteria to concrete techniques, the established recommendations in the literature have been followed (Shenton, 2004); in addition, feedback on the design and findings was obtained from experts working in the field of digital technologies and international relations, drawing on peer review.

The active role of the researcher in the analysis has not been disregarded. In an interpretive study, the findings are not independent of the researcher's point of view; care has therefore been taken to be aware of one's own framing tendencies and to address conflicting geopolitical narratives from as equal a distance as possible. Rather than counting the perspective of China, the West, or Russia as right or wrong from the outset, seeking to understand each within its own logic is the essence of the attitude adopted.

The most sensitive matter from an ethical standpoint is the dual-use nature of the technologies examined. Because cyber capabilities, AI-supported systems, or surveillance tools can be used for both defensive and offensive purposes, the study has carefully refrained throughout from providing functional or technical detail on how these tools might be misused; the focus has been turned toward protective policies and measures against threats. In discussing surveillance and data-collection practices, the international criteria concerning the protection of personal data have been observed; and in the assessment, rather than justifying a particular political stance in advance, an effort has been made to give fair place to different value systems. The clear indication of sources and the rendering visible of the grounds of the inferences have been counted as an inseparable part of the study's scholarly integrity.

Finally, the limits of the method adopted are openly acknowledged. The findings of a qualitative and case-based design cannot be generalized in a statistical sense; but what is aimed at in this study is in any case not statistical but theory-oriented analytical generalization, and the carrying of the findings into other contexts should be assessed on the ground of transferability through thick description. The rapid change of the digital field shortens the period over which the findings remain valid; and the confidential nature of data on states' cyber and intelligence capacities makes it necessary to rely largely on publicly available documents. Since it is known that these documents are at times also used as an instrument for conveying a strategic message, triangulation and

DOI: 10.5281/zenodo.21320691

critical source assessment have been deliberately brought into play to limit the effect of these constraints.

All of these choices are not disconnected from one another; they are parts of a coherent research design that aims to read the transformation digitalization has created in the international system at both the theoretical and the empirical level, without being confined to a single perspective and resting on a sound methodological footing.

5. Findings

With the spread of digital technologies, the center of gravity of the concept of security has shifted from physical geography and classical military capacity toward control over networks, data, and software. States now regard cyber threats not as a secondary matter but as a priority at the center of national security; this orientation is reflected in institutional structures as well. The United States' Cyber Command, China's Cyberspace Force established through the 2024 reorganization, and Russia's cyber-warfare units are concrete signs of the recognition of cyberspace as a separate domain of operations after land, sea, air, and space. This institutional transformation reflects not only a technical specialization but also a reframing of security thinking, because superiority in the cyber domain is measured not by the size of territory or population in the traditional sense but by software competence, intelligence capacity, and infrastructural resilience (Kello, 2017; Segal, 2016).

Whether cyber conflict can be characterized as "war" is one of the oldest and still unresolved debates in the field. Arquilla and Ronfeldt (1993) argued as early as the 1990s that "cyberwar is coming," holding that information superiority would be the decisive element of future conflicts. By contrast, Rid (2013) argued that no cyber incident to date has met the criteria of violence, lethality, and political purpose all at once, and that these should therefore be seen as activities of espionage, sabotage, and disruption rather than war. The tension between these two poles shows that the great majority of cyber incidents are used as an instrument of pressure that remains "below the threshold of war" yet is continuous. Kello (2017) explains this intermediate zone through the concept of the "virtual weapon," drawing attention to the fact that cyber tools can destabilize the international order even without a direct war taking place.

The most distinctive feature separating cyber conflict from traditional conflict is the difficulty of determining the identity of the perpetrator with certainty. This situation, termed the problem of attribution, becomes still more complex because the technical traces of an attack can be redirected toward other actors, proxy groups can be brought into play, and the link between the state and these groups can be deliberately blurred. Maurer (2018) shows that states often use their cyber capacities through proxy actors he characterizes as "cyber mercenaries" rather than directly through their own institutions, and that this facilitates the denial of responsibility. This uncertainty in attribution is not a merely technical matter; since in international law the imputation of an act to a particular state is also decisive in terms of the right to respond arising, it produces direct legal and strategic consequences (Moynihan, 2019).

The examples of the past two decades show how cyber operations turn into an instrument of pressure during periods of crisis. The intensive denial-of-service attacks targeting Estonia's public and banking systems in 2007, the conduct of operations against Georgia in 2008 simultaneously with military operations, and the attacks directed at Ukraine from 2014 onward reveal that digital tools have become an extension of geopolitical tension. Among these examples, the attack on Ukraine's electricity distribution companies in 2015, which left some 230,000 subscribers without power for several hours, is a turning point in that it is the first publicly known case in which a public-service infrastructure was disabled remotely. The fact that the NotPetya attack, which spread worldwide in 2017, caused billions of dollars in damage to logistics, pharmaceutical, and energy companies, and that the ransomware directed at Colonial Pipeline in 2021 disrupted fuel distribution along the east coast of the United States, shows how critical infrastructure can be reduced, with digitalization, to a single point of fracture. Current threat assessments reveal that state-linked actors are increasingly targeting sectors such as energy, health, finance, and public administration (Microsoft, 2025; European Union Agency for Cybersecurity, 2024).

These events have also rendered visible the inadequacy of international law in the cyber domain. Questions such as when a cyberattack will be counted as an "armed attack," under what conditions it will give rise to the right of self-defense, and how proportionate response is to be measured in the digital environment are still contested. Although NATO has declared that a severe cyberattack could be assessed within the scope of Article 5, which governs collective defense, the threshold for applying this framework remains uncertain. The Tallinn Manual 2.0, the most comprehensive academic effort aimed at filling the gap, sets out in detail how the rules of international law in force might be adapted to cyber operations, yet it does not carry the character of a binding treaty and has not attained a shared acceptance among states (Schmitt, 2017; Moynihan, 2019). The recent trajectory of cyber-conflict studies likewise shows that the field is now addressed not merely as a technical security matter but as a multilayered research agenda along the axes of sovereignty, law, and norms (Dunn Cavelty & Wenger, 2024).

The establishment of deterrence in the cyber domain differs structurally from nuclear deterrence. The logic of mutually assured destruction that provides stability in the nuclear field is not directly valid for cyber operations, whose perpetrator cannot be known with certainty, whose effects are scalable, and which are often reversible. States therefore use three complementary approaches together: deterrence by denial, which aims to lower the chance of an attack's success through technical resilience; deterrence by punishment, which threatens retaliation; and normative deterrence, which seeks to define unacceptable behavior through shared norms. Although the processes of the Group of Governmental Experts and the Open-Ended Working Group within the United Nations contribute to this normative framework, deep differences of view persist among states regarding binding rules (Nye, 2011; Kello, 2017).

The entry of artificial intelligence into the cyber domain has turned into an element that continuously reconstructs the balance on both the defensive and the offensive side. While machine-learning-based systems strengthen defense by detecting unusual patterns in network traffic in real time, the same techniques also enable the development of attack tools that automatically scan the vulnerabilities of target systems and can adapt themselves. Current threat assessments show that generative artificial intelligence makes phishing content and social-engineering campaigns more

DOI: 10.5281/zenodo.21320691

convincing, thereby lowering the cost of attack while enlarging its scale (Microsoft, 2025; World Economic Forum, 2026). This trend deepens further with the spread of Internet-of-Things devices and 5G networks, because billions of connected devices produced with weak security standards widen the attack surface. The fact that in 2016 a botnet composed of devices captured by the Mirai malware targeted a major domain-name provider and rendered numerous popular services inaccessible is a concrete example of this vulnerability (DeNardis, 2020; European Union Agency for Cybersecurity, 2025). The debate around the role of particular suppliers in 5G infrastructure, for its part, shows how technological dependence turns into a security and geopolitical matter, pointing to the fact that network infrastructure itself can be used as an instrument of influence and pressure (Bradford, 2023; Farrell & Newman, 2023).

When these developments are assessed together, it becomes clear that cyberspace not only adds a new category of threat to international relations but also changes the basic structural conditions of interaction among states. The growing permeability of borders, the ability of the perpetrator to remain hidden, and the determining role of the private sector over critical infrastructure require a redefinition of the concepts of power and security (Foulon & Meibauer, 2024).

The second major transformation in the field of security is the integration of artificial intelligence into military doctrine and operational capabilities. The great powers have developed strategic concepts that place this technology at the center: the United States' Third Offset Strategy, China's approach of "intelligentized warfare," and Russia's conception of next-generation warfare reveal that future military superiority is directly linked to the capacity for speed, data processing, and automation. Artificial intelligence offers a processing power that exceeds the limits of human capacity in fusing sensor data, in target detection, in logistics planning, and in intelligence analysis (Arsenault & Kreps, 2024; Ndzendze & Marwala, 2023). At the basis of this capability lies the fact that artificial intelligence is essentially a prediction technology; the value it adds to decision-making processes stems from its producing forecasts that reduce uncertainty (Agrawal et al., 2022).

Autonomous weapon systems constitute the most contentious end of this transformation. The distinction made according to the human being's position within the decision loop—systems in which the human makes the decision, supervises it, or is left entirely outside it—lies at the center of the legal and ethical regulation of autonomous weapons. Fully autonomous systems, in which the decision on target selection and engagement is left to the machine, bring to the agenda the application of the principles of distinction and proportionality of international humanitarian law, the question of to whom responsibility will belong in the event of possible violations, and the risk of these systems proliferating to non-state actors (Scharre, 2018). These concerns have been the driving force of the intergovernmental negotiations conducted within the framework of the Convention on Certain Conventional Weapons and of civil-society campaigns; yet a consensus on a binding prohibition has not yet been reached among the major military powers. Data showing that artificial intelligence is rapidly spreading on a global scale likewise confirm that regulatory frameworks lag behind the technology (Stanford Institute for Human-Centered Artificial Intelligence, 2024).

The military value of artificial intelligence is not limited to weapon platforms; it is becoming decisive in intelligence, surveillance, and reconnaissance activities and in command-and-control processes as well. Image-recognition and natural-language-processing techniques can rapidly turn large data sets, from satellite and aerial imagery to open-source intelligence, into meaningful information, thereby providing commanders with a more comprehensive situational awareness in a shorter time. This acceleration brings new risks with it. Biases arising from the data on which algorithms are trained, the fragility they display in unexpected situations, and the weakening of human oversight may lead to erroneous assessments and unintended escalation in moments of crisis. The prospect that, in scenarios where decision time is compressed, AI-supported systems weaken stability by increasing first-strike pressure is a serious source of concern (Bremmer & Suleyman, 2023). Frameworks for the responsible use of artificial intelligence are therefore gaining importance; national guidelines proposing a risk-based management model, multilateral principles, and binding regulatory initiatives are reflections of this search at different levels (National Institute of Standards and Technology, 2023; Organisation for Economic Co-operation and Development, 2019; European Parliament & Council of the European Union, 2024).

One of the technologies that comes to the fore along the axis of data security is blockchain. Distributed-ledger architecture allows data to be verified by the participants in the network and recorded immutably without the need for a central authority. This structure is more resistant to manipulation than traditional databases that are open to attack from a single center; because altering records retroactively requires the capture of a large part of the network, it is in practice extremely difficult. Kshetri (2017) shows that the guarantee of integrity and the transparent verifiability provided by blockchain carry a concrete potential for strengthening cybersecurity and protecting privacy. Permissioned blockchain applications in areas such as identity verification, provenance tracking in the supply chain, and the authorized sharing of sensitive information are the examples closest to the practical realization of this potential.

At the same time, blockchain's promise of security depends on the resilience of the cryptographic foundation it uses, and this foundation is under threat with the development of quantum computing. When a sufficiently powerful quantum computer reaches the capacity to break the RSA and elliptic-curve-based algorithms in widespread use today, not only blockchain systems but a large part of secure communication on the internet will become vulnerable. This forecast has turned the transition to quantum-resistant encryption into an urgent policy priority. The fact that standardization bodies have published the first post-quantum cryptography standards, including lattice-based key-exchange and digital-signature schemes, and have prepared roadmaps for the transition, shows that states take this risk seriously (National Institute of Standards and Technology, 2024a, 2024d; Organisation for Economic Co-operation and Development, 2025). The leap that the combined use of quantum computing with artificial intelligence would provide in intelligence analysis and code-breaking carries this race to a new front of international security (Rodríguez, 2025).

There are also other obstacles before the spread of blockchain in international security applications. The problem of scalability is constraining for public applications in which high volumes of data must be processed; the high energy consumption of systems based

DOI: 10.5281/zenodo.21320691

on the proof-of-work mechanism is criticized in terms of sustainability; and the international incompatibility regarding regulation and standards complicates cross-border applications. Blockchain therefore, while offering a powerful instrument for data security, should be assessed not as a solution by itself but as a complementary component of a broader security architecture (DeNardis, 2020).

Another marked effect of digital technologies on international relations is seen in the scale and sophistication that perception management and disinformation have reached. States no longer limit their information operations to direct propaganda; they turn toward more covert techniques aimed at deepening social polarization, eroding trust in institutions, and blurring the ground of shared reality. Russia's approach to information warfare, China's doctrine of the "three warfares" combining the psychological, public-opinion, and legal dimensions, and various practices of strategic communication are examples of this orientation. Singer and Brooking (2018) show that in this process social media has turned not merely into a medium of broadcast but into an arena in which conflict is itself conducted, and that the mechanisms of likes, shares, and visibility are weaponized.

Artificial intelligence multiplies the effect of disinformation by automating and personalizing it. Deepfake technologies can produce video and audio recordings that make publicly recognized figures appear to say things they never said; distinguishing the authenticity of such content is becoming increasingly difficult. In 2018, a production team's sample video imitating former US President Barack Obama showed the public the point the technology had reached. That this capacity could turn into an instrument of international crisis became clearly apparent during Russia's invasion of Ukraine in 2022: a fake video spread through a hacked news channel showing President Volodymyr Zelensky calling on his soldiers to surrender went down as the first example of the deliberate use of a deepfake in an active armed conflict. Although the footage was quickly debunked and removed, it laid bare the confusion and the erosion of public trust that such a tool could create in a moment of crisis. The ability of generative text models to produce content hard to distinguish from a human pen, for its part, enlarges the scale of campaigns by enabling a small number of operators to create large numbers of fake accounts and content; this trend also coincides with current assessments that generative artificial intelligence both cheapens and disseminates disinformation (World Economic Forum, 2026).

The real mechanism that makes this content effective is micro-targeting. Big data and machine learning allow messages tailored to individuals' demographic, psychological, and behavioral profiles to be delivered to particular audiences. The Cambridge Analytica case clearly revealed how personal data gathered through social media could be used for the purpose of psychological profiling aimed at influencing voter behavior. Zuboff (2019) shows that behind these practices lies an economic logic in which user behavior is monitored in detail, turned into prediction products, and marketed; that this order, which she terms "surveillance capitalism," prepares the ground not only for commercial but also for political manipulation (Fuchs, 2021).

The very functioning of social media platforms also facilitates disinformation. Algorithms designed to maximize engagement bring to the fore content that arouses emotional reaction and is polarizing; echo chambers and filter bubbles reinforce social division by confining users to content that confirms their own views. A large-scale study revealed that false news spreads faster, wider, and deeper on social networks than true news (Vosoughi et al., 2018). Networks of bots and coordinated inauthentic behavior distort public debate by artificially pushing particular content onto the agenda. Platforms' decisions regarding content moderation, for their part, create a new form of private authority that determines which speech will be visible, and the accountability of this authority constitutes a governance problem in its own right (Gorwa, 2019; Castells, 2015).

In countering disinformation, technological, regulatory, and educational tools are used together. The European Union's Digital Services Act and its code of practice on disinformation are among the most comprehensive regulatory initiatives that impose obligations of transparency and content moderation on platforms (Bradford, 2023). Independent verification organizations, deepfake-detection technologies, and media-literacy programs complement this effort. Yet as the race between production techniques and detection methods continues, it becomes clear that technical or regulatory solutions alone are not sufficient, and that more fundamental approaches, such as strengthening critical thinking and institutional trust, remain decisive.

On the economic plane, the most visible effect of digitalization is the erosion of states' control over money and payment systems. The emergence of crypto assets such as Bitcoin and Ethereum has led to the development of a parallel financial ecosystem operating without the need for a central authority; decentralized finance protocols built on smart contracts have begun to offer disintermediated versions of traditional banking functions such as lending, the provision of liquidity, and asset management. While these structures carry the promise of accelerating cross-border transactions and lowering costs, they strain states' capacity for control in the areas of money laundering, the financing of terrorism, and taxation. The fact that most decentralized protocols do not apply know-your-customer and anti-money-laundering obligations creates a serious gap for regulatory institutions (Organisation for Economic Co-operation and Development, 2024).

States respond to this development by developing digital currencies under their own control. China's digital yuan, the European Central Bank's work on a digital euro, and Sweden's e-krona project are prominent examples of central bank digital currencies. These initiatives, besides offering a state-controlled alternative to decentralized crypto assets, also serve such aims as adapting monetary policy to the digital age, efficiency in payments, and combating financial crime. China's step is at the same time read as a strategic move aimed at reducing dependence on the dollar in international payments (Bank for International Settlements, 2021). In the design of these currencies, the balance between privacy and auditability is foremost among the most debated issues.

The most direct effect of digital currencies on international relations arises in the field of economic sanctions and financial surveillance. Farrell and Newman (2023) show that the United States has turned its central position in global payment and banking networks into a weapon of foreign policy; that by controlling access to infrastructures such as SWIFT it can exert pressure on its rivals. That states subject to sanctions turn toward crypto assets and alternative payment systems is a result of the search to limit the effect of this weapon. While this trend creates a medium-term challenge to the privileged position of the dollar and the effectiveness of sanctions, the regulation of decentralized and

DOI: 10.5281/zenodo.21320691

cross-border structures stands as an unresolved problem for international regimes of financial oversight.

The same technologies also offer an opportunity in terms of financial inclusion. Worldwide, around 1.4 billion adults still cannot access basic financial services (World Bank, 2022). Mobile money and digital payment systems carry the potential to close this gap in regions where banking infrastructure is inadequate; the M-Pesa system developed in Kenya, by including millions of people in the formal financial system, constitutes the best-known example of this. The fact that the average cost of cross-border money transfers, according to World Bank data, still runs above six percent and remains behind the three-percent threshold of the Sustainable Development Goals lends meaning to the cost-reducing promise of digital solutions. Still, the realization of this potential depends on conditions such as digital literacy, reliable connectivity, and user protection; otherwise the same technologies may reinforce existing inequalities.

The maturation of the digital-asset ecosystem depends on the development of regulatory frameworks. Initiatives such as the European Union's Markets in Crypto-Assets regulation aim to strengthen both investor protection and market stability by increasing legal certainty in this field (Bradford, 2023). The basic tension of regulation is, on the one hand, to provide the oversight that will prevent abuse, and on the other, not to stifle the cross-border and innovation-open nature of these technologies.

The legal and normative dimension of digital transformation becomes most clearly visible in the field of digital rights. The resolution adopted by the United Nations Human Rights Council in 2012, by affirming that the rights valid in the offline environment require the same protection in the online environment, has been a turning point in the formal recognition of this field within the international human rights framework (United Nations Human Rights Council, 2012). Rights such as internet access, privacy, freedom of expression, and access to information have, with digitalization, both acquired new safeguards and encountered new threats.

The most influential regulatory model in this field is the European Union's General Data Protection Regulation. This framework, which grants the individual rights such as erasure, portability, and explicit consent over their data, has inspired regulations in different regions of the world, notably in California and Brazil. Bradford (2023) shows that, thanks to its market size and regulatory capacity, the European Union is able to impose its own standards indirectly on a global scale; that through this mechanism, which she terms the "Brussels effect," the rules of the digital field are shaped to a significant degree in a Europe-centered manner. Yet the difference between approaches that grant technology companies a wider field of movement and data-protection regimes that place the individual at the center is the principal obstacle before a global standardization.

The spread of artificial intelligence and algorithmic decision-making systems has opened a new problem area in terms of digital rights. Used in processes that directly affect the individual's life, such as credit, employment, social assistance, and criminal justice, these systems carry the risk of reproducing the biases in the data on which they are trained. The investigation regarding the COMPAS risk-assessment tool used in the criminal-justice process in the United States, which found that it produced biased results against Black defendants, is a concrete example of this risk (Angwin et al., 2016). In response to these concerns, the European Union's regulation, which classifies artificial intelligence systems according to risk levels and imposes strict obligations on high-risk applications, has the character of the first comprehensive legal framework on a global scale (European Parliament & Council of the European Union, 2024). UNESCO's recommendation on the ethics of artificial intelligence and the United Nations' high-level report addressing the governance of artificial intelligence for the benefit of humanity likewise set out common principles for the development of these systems in a manner respectful of human rights (UNESCO, 2021; High-Level Advisory Body on Artificial Intelligence, 2024).

The spread of digital surveillance constitutes the heaviest pressure on the right to privacy. The documents that Edward Snowden disclosed to the public in 2013 laid bare states' capacity for mass communications surveillance; China's social-credit applications and the intensive surveillance practices in the Xinjiang region, for their part, showed that digital technology can turn into an instrument of social control. The Big Brother Watch and Others judgment delivered by the Grand Chamber of the European Court of Human Rights in 2021, by subjecting the compliance of mass communications interception with human rights standards to judicial review, established that surveillance programs—even those conducted on grounds of national security—must be limited by independent oversight and legal safeguards (European Court of Human Rights, 2021). The data-collection and profiling practices of the private sector have likewise become as decisive as state surveillance in terms of privacy (Zuboff, 2019).

Freedom of expression and access to information have, in the digital environment, both expanded and encountered new restrictions. States' practices of internet censorship, content blocking, and network shutdowns directly restrict these rights, while the comprehensive filtering systems of some countries constitute the most developed example of this. Independent assessments reveal that only a small portion of the world's population lives in a fully free internet environment (Freedom House, 2024). In this picture, not only states but also the large platforms that, through their content-moderation decisions, determine the visibility of billions of users are an influential actor; the protection of freedom of expression therefore requires an understanding of responsibility encompassing both public and private authority (Gorwa, 2019).

Inequality in access to digital rights is a problem of justice in its own right. According to the data of the International Telecommunication Union, in 2024 about one-third of the world's population, numbering 2.6 billion people, is still offline; while this rate reaches ninety-three percent in high-income countries, it remains at twenty-seven percent in low-income countries (International Telecommunication Union, 2024). The differences in access between urban and rural areas and between women and men carry existing inequalities into the digital field. In a world where education, health, and public services are increasingly moving online, this gap carries the risk of deepening the deprivation of disadvantaged groups. The United Nations' development agenda therefore defines the provision of universal and meaningful connectivity as a priority goal (United Nations, 2021).

All of these developments lead states to develop differing conceptions of sovereignty regarding the digital field. The questions of where data will be stored, how cross-border flows will be regulated, and by whom digital infrastructure will be controlled

DOI: 10.5281/zenodo.21320691

are the subject of a debate that is both normative and geopolitical. The concept of digital sovereignty itself is defended in some approaches as a legitimate instrument for the protection of the individual and society, while in some cases it can turn into a discourse that legitimizes control and closure (Roberts, 2024; Braun & Hummel, 2025; Glasze et al., 2023). The divergence around this concept leads states to adopt diverging choices across a broad field, from AI governance to data regulation, and causes the global digital order to acquire a fragmented appearance (Mügge, 2024; Srivastava & Bullock, 2024).

When these findings are assessed as a whole, it becomes clear that digital technologies do not merely change the international system in individual fields but transform it through the intersections that connect these fields to one another. Although cybersecurity, artificial intelligence, blockchain, quantum computing, digital money, and digital rights can be examined under separate headings, in practice they form an interwoven whole: quantum computing affects both encryption and blockchain, artificial intelligence strengthens both military capacity and disinformation, and control over data has an economic and a security dimension at the same time. This intersectional structure renders permeable the boundaries among security, economics, and law, and carries competition among states onto a multilayered ground. The findings obtained reveal that digitalization does not merely add new instruments but at the same time reconstructs the framework within which power, sovereignty, and security are defined, and they prepare the ground for the theoretical assessment to be addressed in the following section.

6. Discussion

When the findings of this study are read together, headings such as the routinization of cyber conflict, the embedding of AI-supported systems into defense and intelligence practices, the unsettling of the encryption order by quantum computing, the loosening of the instruments of financial control by blockchain and digital currencies, the changing of forms of negotiation by digital diplomacy, and the triggering by digital rights of a normative transformation in international law appear not as disconnected developments but as parts of a common pattern. This pattern shows that digitalization is not a topic added later onto international relations but a process that re-layers the basic grammar of power, security, and sovereignty. Traditionally, a state's weight was measured through territory, population, army, and national income; the distinction between the hard and soft forms of power also rested largely on this material basis (Nye, 2011). The findings, however, reveal that stocks of data, computing capacity, algorithmic superiority, and infrastructural control do not replace the old criteria but settle upon them like a new layer and recode them all. Drezner (2019) recalls the discipline's tendency to see every technological wave as either a revolution that changes everything or a detail with no noteworthy novelty; the results here stand precisely between these two poles. In the environment Floridi (2014) terms the infosphere, the boundary between online and offline in politics, economics, and conflict is increasingly blurring, and this requires the recalibration of the concepts at international relations' disposal.

The findings on the field of security acquire meaning best when placed within the decades-long debate over the nature of cyber conflict. Arquilla and Ronfeldt (1993) early declared that a cyberwar was approaching, while Rid (2013), opposing this, argued that no cyberwar in the genuine sense would take place and that what was observed fell into the categories of sabotage, espionage, and disruption. The findings of this study support a reading midway between the two: Kello's (2017) conceptualization of the virtual weapon and a state of tension remaining between peace and war, together with Buchanan's (2020) definition of cyber operations not as war but as a permanent form of geopolitical competition conducted below the threshold, fit the observed pattern better. Segal (2016) names this new order a hacked world order and shows that states no longer merely fight but also trade, maneuver, and steer one another with digital tools, so that the line between security and economics becomes blurred. Indeed, studies assessing the field's own historical trajectory likewise reveal that cyber-conflict research has shifted from a categorical debate about war to an analysis of everyday and continuous competition (Dunn Cavelty & Wenger, 2024). Foulon and Meibauer (2024) argue that cyberspace functions less as something that transforms the international system on its own than as a modifier that accelerates or slows existing structural tendencies; this also helps explain why the findings point to a gradual reshaping rather than a wholesale rupture.

The concrete appearance of the cyber-threat environment offers an empirical ground that supports this theoretical reading. The annual assessments of the European Union Agency for Cybersecurity document that ransomware attacks, supply-chain intrusions, and state-linked operations are now not the exception but an ordinary background noise (European Union Agency for Cybersecurity [ENISA], 2025). Similarly, threat reports originating from the private sector and the assessments of international organizations reveal that the boundary between state-sponsored actors and crime networks is blurring (Microsoft, 2025; World Economic Forum, 2026). This landscape carries the problem of attribution and the applicability of international law to the center of debate. The Tallinn Manual work offered a framework by elaborating how existing international law might apply to cyber operations (Schmitt, 2017), yet it has been shown that the limits of the violation of sovereignty and the principle of non-intervention in the cyber context are still contested (Moynihan, 2019). Maurer's (2018) concept of cyber mercenaries, for its part, explains how states' monopoly over the instruments of violence is loosening and how deniable operations are made possible through proxy actors. When these phenomena are brought together, it becomes clear why traditional deterrence theory is strained in the cyber domain: in an environment where the perpetrator cannot be determined with certainty, where the threshold is continuously eroded, and where the cost of retaliation cannot be foreseen, the logic of stability inherited from the Cold War does not directly operate. Deterrence is partly being replaced by strategies of wearing down the adversary through resilience and continuous contact.

The effect of artificial intelligence reflected in the findings sharpens the tension between power and governance. Bremmer and Suleyman (2023) term this situation a paradox: states must govern artificial intelligence without delay, yet the greater part of the capacity is concentrated not in states' hands but in a limited number of companies. Arsenault and Kreps (2024), together with Ndzendze and Marwala (2023), addressing how artificial intelligence is incorporated into international relations theories, show that the technology behaves like a capability multiplier and can widen existing power differences rather than close them. On the economic plane, Agrawal et al. (2022) reveal that artificial intelligence is in essence a technology that lowers the cost of prediction, and that

DOI: 10.5281/zenodo.21320691

cheaper prediction reshapes not only markets but also decision-making processes such as military targeting, intelligence analysis, and crisis management. The question of how this capacity is to be directed has led to the emergence of fragmented and competing regulatory initiatives. While the European Union's risk-based approach has turned into binding legislation (European Parliament & Council of the European Union, 2024), voluntary principles and frameworks continue to function alongside it (Organisation for Economic Co-operation and Development [OECD], 2019; National Institute of Standards and Technology [NIST], 2023). The search for harmonized governance on a global scale, for its part, is still at an initial stage (High-Level Advisory Body on Artificial Intelligence, 2024). The geographic and institutional concentration of capacity is confirmed by independent measurements as well: leading models, computing infrastructure, and expert human resources are seen to cluster in particular countries and companies (Stanford Institute for Human-Centered Artificial Intelligence, 2024). Viewed from a constructivist standpoint, it may be said that concepts such as trustworthy artificial intelligence or AI safety are themselves norms not yet settled, constructed contentiously among actors.

The findings on autonomous systems constitute the field in which this tension between power and governance is seen most sharply. The acceleration of the decision loop tends to shift the human role, in the process extending from target detection to engagement, from being a decision-maker to being a supervisor; whereas the preservation of meaningful human control remains critical both for legal responsibility and for the prevention of escalation. The working of AI-supported systems as a capability multiplier (Arsenault & Kreps, 2024) also brings with it the risk that decision speed destabilizes the deterrence balance: in an environment where machines respond to one another within seconds, an escalation arising from misperception may occur before there is an opportunity for human negotiation to come into play. The logic of below-threshold competition that Buchanan (2020) described for cyber operations becomes still finer in autonomous systems, because deniability and uncertainty intensify as the level of autonomy increases. As Bremmer and Suleyman (2023) warn, governance lagging behind technological development in this field may create faits accomplis that, once established, are difficult to reverse; the adaptation of the logic of arms control to digital and autonomous capacities is therefore one of the principal questions of the future architecture of international security.

The findings on quantum technologies have a distinct importance in terms of changing the temporal dimension of security. The prospect of the spread of quantum computers turns the expectation that data captured today in encrypted form could be broken in the future—that is, the "harvest now, decrypt later" logic—into a threat already now. For this reason, standard-setting bodies have published the post-quantum algorithms that will replace classical encryption even before quantum computers have matured, and have declared a transition timetable (NIST, 2024a, 2024b, 2024c, 2024d). Although at the policy level the security and competition dimensions of quantum technologies are not yet mature, they are rapidly settling onto the agenda (OECD, 2025). Moreover, the combined use of quantum with artificial intelligence may increase both offensive and defensive capacities in a mutually reinforcing way (Rodríguez, 2025). The real issue here is not merely technical: because whoever writes an encryption standard also determines what rules others will follow, the standard-setting process itself turns into a structural form of power. In this respect, the transition to quantum is less a problem of technical adaptation than an arena of competition over whose standard will be valid on a global scale, and in this respect it is directly akin to the logic of chokepoint control in financial and information networks.

The economic findings expose the two-sided nature of digital finance, which is at once decentralizing and productive of new dependencies. On the surface, central bank digital currencies and decentralized finance appear to distribute power by reducing intermediaries. Yet, as Farrell and Newman (2023) show, global finance and information networks are organized around certain nodal points, and the states controlling these chokepoints can turn interdependence into an instrument of pressure; payment-messaging systems, dollar clearing, and cloud infrastructure are typical examples of this. Central bank digital currencies are designed to operate alongside cash in a two-tier structure and observe a balance between privacy and integrity (Bank for International Settlements, 2021). Blockchain, for its part, while carrying the promise of increasing security and transparency, also brings with it its limits in terms of scalability and oversight (Kshetri, 2017). These findings reveal how Keohane and Nye's (2012) theory of interdependence must be reread in the digital age: while symmetric dependence feeds cooperation, asymmetric dependence turns directly into a lever of coercion. The question of in whose hands the gains accumulate has also not been closed; it is emphasized that technological change does not spread prosperity by itself and that distribution remains tied to institutional and political choices (Acemoglu & Johnson, 2023). Early studies on the fourth industrial revolution and the second machine age had foregrounded the productivity dimension of this transformation (Schwab, 2016; Brynjolfsson & McAfee, 2014); current assessments, for their part, render more visible the problems of inequality and governance that the growth of the digital economy brings with it (OECD, 2024).

The findings on digital diplomacy show that technology, rather than reinventing diplomatic practice in its entirety, transforms deep-rooted functions such as representation, communication, and negotiation. Bjola and Holmes (2015) propose addressing digital diplomacy as a process of change management rather than a revolution; this framework is more productive than a determinist reading in explaining the digital–analog hybridization observed in the findings. Social media platforms have become for foreign-affairs institutions both a stage on which public diplomacy is conducted and a data source through which interaction can be measured; the communication logic of the network society determines how messages spread on this stage and how coalitions are formed (Castells, 2015). AI-supported analytical tools support negotiation preparation and crisis management by processing large volumes of data, but at the same time give rise to new ethical challenges such as algorithmic bias and problems of transparency. The nature of diplomacy is thus shifting toward a new balance among openness and secrecy, speed and restraint, automation and human judgment; this balance constitutes the principal agenda of the adaptation of traditional diplomatic institutions to the digital age.

The findings on perception management and disinformation point to an epistemic threat field where security and diplomacy intersect. Singer and Brooking (2018) show that social media has turned into a weapon, and that conflicts are now conducted not only over territories but also over attention and credibility. In this environment, information itself becomes a battlefield, and states

DOI: 10.5281/zenodo.21320691

seek to shape public perception through proxy actors and automated accounts. The horizontal and rapid-spread logic of the network society produces both a democratizing capacity for mobilization and a vulnerability open to manipulation (Castells, 2015). Critical media studies reveal that this vulnerability is not incidental; that the attention economy and data-driven targeting structurally reward polarizing and emotional content (Fuchs, 2021). The conclusion that follows is that social trust and a shared factual ground themselves become a source of security; what disinformation erodes is not merely a particular political outcome but a society's capacity to agree on a shared reality.

The findings under the headings of platform power, digital sovereignty, and governance can be interpreted most productively within the framework of competing regulatory orders. Bradford (2023) argues that global technology governance is shaped around three distinct imperial models: the market-driven American model, the state-driven Chinese model, and the rights-driven European model. This threefold distinction renders the rival rule-setting efforts observed in the findings intelligible under a single roof. At the same time, the concept of digital sovereignty itself is normatively slippery; it is often reduced to a one-dimensional and overly simplified idea of control (Braun & Hummel, 2025). It has been shown that the concept functions as a political discursive practice rather than a legal category (Glasze et al., 2023), that it remains normatively inadequate when defined as mere control (Roberts, 2024), and that in the European case it becomes unclear precisely for whose benefit it operates (Mügge, 2024). The governance of platforms has become a problem area in its own right (Gorwa, 2019), and with the embedding of the internet in every corner of everyday life, a dependence with no off switch has emerged (DeNardis, 2020). The turning of user data by large technology companies into a source of capital accumulation has been analyzed in detail within the framework of surveillance capitalism and critical media studies (Zuboff, 2019; Fuchs, 2021). At this point, Srivastava and Bullock's (2024) emphasis on the interweaving of public and private power is important: companies are not taking the place of states but are embedded in global governance in both cooperation and contention with states. Analyses of the network society (Castells, 2015) and the search for a multistakeholder global agenda (United Nations, 2021) constitute the theoretical and institutional background of this interwoven structure.

The findings on digital rights point to a silent but deep normative shift in international law. The fact that concepts such as data sovereignty, algorithmic transparency, and the ethics of artificial intelligence have become new parameters of global governance shows that rights are being redefined not only among states but also in the relationship among state, company, and individual. Floridi (2018) argues that in this field rules alone are not sufficient; that, beyond the minimal framework drawn by legislation, a soft-ethics approach is needed that asks not only what can be done but also what ought to be done. This approach is consistent with analyses that seek to construct digital sovereignty not as mere control but as a normative responsibility that observes rights (Roberts, 2024; Braun & Hummel, 2025). At the European level, early policy documents that observe excellence and trust together (European Commission, 2020) are part of an effort to institutionalize an understanding of artificial intelligence that places human dignity at the center; on a global scale, the search for governance for the benefit of humanity (United Nations, 2021; High-Level Advisory Body on Artificial Intelligence, 2024) and common principles among states (OECD, 2019) are attempts to carry this normative framework to the international level. The findings reveal that these initiatives still advance in a fragmented and mutually contending manner, and that the becoming of digital rights into a universal regime is therefore not a technical but a political matter.

When all these findings are assessed together, the question of which theoretical approach better explains digital transformation is not closed by an answer given to a single tradition. Technological determinism assumes that technology determines societies through its own internal logic and therefore underestimates states' choices, institutions' resistance, and the contentious construction of norms. Pure constructivism, for its part, rightly foregrounds the social construction of meanings and norms, but carries the risk of not taking sufficiently seriously the constraining weight of material layers such as computing power, fiber infrastructure, and data centers. The analysis of this study argues that a sociotechnical and network-relational reading standing midway between the two, in which technology and society mutually produce each other, is more explanatory. In such a reading, realism's emphasis on power projection is preserved, but the weight of non-state actors is rendered visible; liberal theory's grasp of interdependence is maintained, but the point that this dependence can be weaponized is added; constructivism's emphasis on norm contention is adopted, but the material limits of infrastructure and computing capacity are not overlooked. Floridi's (2014) infosphere and Castells's (2015) network logic provide the principal theoretical supports of this synthesis; analyses of cyber politics also offer an early but still productive framework for understanding states' behavior in the digital environment (Choucri, 2012).

This study has certain limitations, and setting them out clearly is necessary in order to assess to what extent the results can be generalized. First, the speed at which the examined technologies develop increases the likelihood that a portion of the findings will quickly lose currency; assessments valid today, especially in the fields of artificial intelligence, quantum computing, and digital finance, may require reexamination within a few years. Second, the fact that states keep largely confidential their data on cyber operations, intelligence activities, and defense capacities limits empirical depth in these areas and confines the analysis to publicly available documents and expert assessments; these sources, in turn, do not always reflect actors' real intentions and implicit strategies. Third, the focus of the study lies heavily on the strategies of great powers such as the United States, China, Russia, and the European Union; this gives rise to the risk that the experiences of Global South countries are not sufficiently represented. The point to be noted here is that the digital divide is not merely a gap arising from a research choice but a real and measurable inequality; the differences in access, infrastructure, and skills between developed and developing countries are documented by independent analyses (OECD, 2024). Fourth, because the study's method is largely qualitative and interpretive, the quantitative measurement of effects and the definite determination of causal relations become difficult. Finally, the theoretical tension between technological determinism and social constructivism is not entirely resolved in this study; although the sociotechnical reading adopted seeks to manage this tension, it offers a productive middle path rather than a definitive consensus.

That the findings are open to alternative readings enriches the debate rather than weakening the strength of the results. The first

DOI: 10.5281/zenodo.21320691

alternative explanation argues that digital technologies, rather than transforming the international system, reproduce existing hierarchies. According to this view, because advanced artificial intelligence and big-data analysis require considerable capital, technical expertise, and data, they provide an advantage to the countries and companies that already possess these resources; indeed, the concentration of capacity supports this tendency (Stanford Institute for Human-Centered Artificial Intelligence, 2024). The critical and surveillance-capitalism literature shows that the commodification and control of data reinforce existing power relations (Zuboff, 2019; Fuchs, 2021); analyses arguing that digital sovereignty functions as a discursive practice can be read in the same direction (Glasze et al., 2023). Within this framework, technological dependence is interpreted as a new form of dependency and colonialism, and the map of regulatory empires drawn by Bradford (2023) directly links the question of who sets the rules with the concentration of power. The second alternative explanation, by contrast, runs in the opposite direction and argues that digitalization horizontalizes power and strengthens non-state actors. When the increasing weight of companies, civil-society networks, and proxy actors (Srivastava & Bullock, 2024; Gorwa, 2019; Maurer, 2018) is combined with the network society's capacity for horizontal mobilization (Castells, 2015), the conclusion can be reached that power has moved out of states' monopoly and taken a more dispersed form. These two readings do not exclude each other; on the contrary, they suggest that the same process produces both concentration and dispersion simultaneously at different layers.

Within this framework, the very tension between transformation and reproduction can be assessed as a finding in its own right. Digital technologies are in essence neither saviors nor destroyers; their consequences depend on how they are designed, under whose control they are developed, and by what norms they are regulated. The form the global system will take will therefore be a result less of the internal logic of technology than of the governance choices that states, international organizations, companies, and civil society will make. Whether interdependence will be a ground of cooperation or a lever of pressure (Farrell & Newman, 2023), whether AI capacity will be bound to accountable rules or will concentrate without oversight (Bremmer & Suleyman, 2023), and whether the discourse of digital sovereignty will evolve into an inclusive rights regime or an inward-looking search for control (Braun & Hummel, 2025) will be determined by these choices. The analysis of this study reveals that a single theoretical tradition is not sufficient to understand the digital age, and that an integrated framework that addresses the material, institutional, and discursive layers of power together is necessary. In the conclusion, the theoretical and political consequences of this framework will be compiled, and the questions opened up for future research will be discussed.

7. Conclusion and Recommendations

The point of departure for this study was the question of the extent to which, and in what direction, digital technologies are transforming international relations along the axes of security, economics, and diplomacy. The analysis has largely confirmed the three central expectations set out at the outset, yet it has qualified each of them in important ways. First, digitalization was found to alter the balance of power; however, this change has taken the form not of a rupture in which states are wholly displaced by new actors, but of a layering in which new resources such as data, algorithms, and network control are added alongside the classical components of power. Second, the centrality of cyber conflict to the security agenda was confirmed; yet rather than substituting for traditional military force, it has opened a plane that complements and complicates it. Third, blockchain and digital-currency technologies were found to exert a marked pressure on international trade and finance; but this pressure reshapes states' monetary control rather than eliminating it. Taken together, the study demonstrates that digitalization is not a unidirectional and inevitable technological advance within the international system, but a multilayered process whose outcome is not predetermined and which is interwoven with political choices, economic interests, and societal values.

The findings on security indicate that cyber conflict has settled in as an enduring arena of contestation. Events such as the large-scale attacks directed at Estonia in 2007, the disabling of Ukraine's electricity grid in 2015, and the ransomware attack on Colonial Pipeline in 2021 have plainly revealed how modern societies' dependence on digital infrastructure has turned into a strategic vulnerability. What these incidents share is that they transcend borders, that their sources frequently cannot be determined with certainty, and that their effects can be disproportionate. These features make it necessary to rethink established concepts such as deterrence and retaliation. The roots of this debate reach back to early work that anticipated cyber struggle would transform the nature of war (Arquilla & Ronfeldt, 1993) and to critical approaches questioning whether such actions can be considered war in any genuine sense (Rid, 2013). Subsequent literature has treated cyberspace as a factor that modifies state behavior within the existing international structure (Kello, 2017; Foulon & Meibauer, 2024) and has documented the maturation of cyber-conflict studies into an established subfield (Dunn Cavelty & Wenger, 2024). The rising frequency and cost of threats to critical infrastructure in recent years can likewise be tracked, year on year, in independent threat assessments (European Union Agency for Cybersecurity [ENISA], 2024, 2025; Microsoft, 2024, 2025; World Economic Forum, 2025, 2026).

The most intractable aspect of this picture is the difficulty of identifying the perpetrators of attacks. The proliferation of proxy actors operating on behalf of states, of hackers-for-hire, and of loosely affiliated online communities renders the assignment of responsibility still more complex (Maurer, 2018). This uncertainty in attribution points to an order in which states can penetrate one another's systems without openly accusing each other, and in which the rules are drawn largely by the prevailing balance of de facto power (Segal, 2016). The same uncertainty also complicates the adaptation of international law to the cyber domain. It remains unsettled under what conditions a cyberattack would count as an armed attack, when it would give rise to the right of self-defense, and how the principle of proportionality is to be applied. The Tallinn Manual offered a comprehensive framework for how existing legal rules might be interpreted with respect to cyber operations (Schmitt, 2017), and the limits of the principles of sovereignty and non-intervention in this context have been examined in detail (Moynihan, 2019). Nevertheless, the binding force of these frameworks is limited and they have not crystallized into a shared consensus among states; the result is the slow development of norms of responsible state behavior and an increase in operations conducted in the gray zone.

The entry of artificial intelligence into military and intelligence processes accelerates decision-making while deepening problems

DOI: 10.5281/zenodo.21320691

of oversight and accountability. The distinction between the human being situated in, on, or out of the decision loop lies at the heart of the debate over autonomous weapons; for as target selection and attack decisions are delegated to the machine, it becomes harder to apply the principles of distinction between combatants and non-combatants and of proportionality, and to ensure accountability for possible violations. Studies addressing the implications of artificial intelligence for international relations theory emphasize that the technology is not merely a tool but a factor that shapes actors' preferences, the distribution of power, and threat perception (Ndzendze & Marwala, 2023; Arsenault & Kreps, 2024). At the same time, the gap between the pace of technological development and the capacity to govern it stands out as a structural problem that hampers oversight (Bremmer & Suleyman, 2023). The rapid advance of these capabilities and the trajectory of investment are likewise documented, year on year, in comprehensive reports that monitor the field (Stanford Institute for Human-Centered Artificial Intelligence, 2024). The decisive effect of artificial intelligence on security will therefore arise not from technical superiority alone, but from whether that superiority can be balanced by institutional oversight and legal frameworks.

Quantum computing adds a medium-term yet fundamental dimension to the security debate. The prospect that sufficiently powerful quantum computers could break the public-key encryption methods in widespread use today already places long-lived confidential data at risk. The expectation that encrypted data captured today could be decrypted in the future means that the threat can no longer be deferred. For this reason, standard-setting bodies have begun the transition process by converting post-quantum encryption algorithms into formal standards (National Institute of Standards and Technology [NIST], 2024a, 2024b, 2024c) and have set out a clear roadmap for the gradual migration of critical systems to these standards (NIST, 2024d). Assessments addressing the policy dimensions of quantum technologies draw attention to the dual nature of the field, which contains both opportunity and threat (Organisation for Economic Co-operation and Development [OECD], 2025); and the compound effects that this technology may produce for cybersecurity when used together with artificial intelligence are also under discussion (Rodríguez, 2025). The race for quantum supremacy is thus turning into a critical arena of competition that will determine future balances of intelligence and defense.

On the economic plane, the findings show that digital value-transfer instruments are eroding states' capacity for monetary control and for the imposition of sanctions. Although the contributions of blockchain in the domain of security and data integrity have been documented (Kshetri, 2017), it remains uncertain in which direction this technology will evolve amid the competition between central bank digital currencies and decentralized finance. China's digital-yuan initiative, the search for alternative payment channels by countries under sanctions, and the growth of crypto assets have brought to the fore debates over the privileged status of the US dollar and the effectiveness of sanctions. This competition is not a purely technical choice; it is a struggle over monetary sovereignty, financial control, and reserve-currency status. In the same period, the conversion of economic networks into instruments of coercion reveals that control over payment infrastructures and supply chains has become a source of power in its own right (Farrell & Newman, 2023). The expansion of the digital economy (OECD, 2024) raises, alongside gains in productivity, the question of who benefits from those gains; studies on the effects of artificial intelligence and automation on labor and the distribution of welfare remind us that the gains may be distributed unequally and may generate new dependencies (Brynjolfsson & McAfee, 2014; West, 2018; Agrawal et al., 2022; Acemoglu & Johnson, 2023).

Perception management and disinformation constitute one of the most tangible risks that digitalization poses to democratic processes. The attention-driven operation of social media platforms facilitates the rapid spread of polarizing content, while AI-enabled synthetic audio and video together with data-driven individual targeting render manipulation more subtle and harder to detect. This phenomenon is closely related to work showing that user data has been transformed into a new mode of capital accumulation (Zuboff, 2019; Fuchs, 2021) and to the platform-governance literature demonstrating that platforms have become de facto regulators of the public sphere (Gorwa, 2019; DeNardis, 2020). The broader framework concerning how information flows are organized in the network society also contributes to understanding the origins of this process (Castells, 2015). In this situation, countering disinformation cannot be reduced merely to the case-by-case moderation of content; it requires a holistic approach that addresses platforms' business models, their data-collection practices, and their accountability together.

All of these tendencies reopen the question of what state sovereignty means in the digital domain. The power of large technology companies to control data, infrastructure, and technical standards increases the weight of non-state actors within the international system. In this context the concept of digital sovereignty has come to the fore both as a policy discourse and as an analytical tool (Glasze et al., 2023; Braun & Hummel, 2025); and in the case of the European Union in particular, the question of for whose benefit and to what end this discourse is deployed has been interrogated (Mügge, 2024). The divergence of regulatory approaches around market-oriented, state-oriented, and rights-oriented models increases the risk of fragmentation of the global internet (Bradford, 2023). Studies that address the relationship between artificial intelligence and sovereignty from a normative standpoint (Roberts, 2024; Srivastava & Bullock, 2024), together with assessments examining the structural effects of technological change on international relations (Drezner, 2019; Choucri, 2012), show that this divergence is not merely technical but a normative competition over whose values the rules of the future will be set by.

The domain of digital rights is a terrain on which a slow but distinct normative development is taking place in international law. Headings such as data protection, algorithmic transparency, and the ethics of artificial intelligence have become new items on the agenda of global governance. Among the steps taken in this direction are the adoption of international principles concerning artificial intelligence (OECD, 2019), the opening to debate of policy frameworks grounded in trust and excellence (European Commission, 2020), the development of risk-based regulatory models (NIST, 2023; European Parliament & Council of the European Union, 2024), and the preparation of comprehensive reports on the governance of artificial intelligence for the benefit of humanity (High-Level Advisory Body on Artificial Intelligence, 2024; United Nations, 2021). These initiatives signal that the ethical and legal foundations of the digital domain must be established not by a single state or a single company, but through a multistakeholder process; the rethinking of moral and legal

DOI: 10.5281/zenodo.21320691

frameworks together with technology in the information age is likewise an inseparable part of this process (Floridi, 2014, 2018).

The theoretical contribution of this study lies in bringing the foregoing findings together within a single framework and thereby moving digital transformation from the margins to the center of international relations theory. Without succumbing to the enthusiasm of popular narratives that present technology as an absolute rupture (Schwab, 2016), and without rejecting the conceptual legacy of the classical approaches to power and interdependence (Keohane & Nye, 2012; Nye, 2011), the study proposes to extend that legacy so as to encompass new sources of power such as the command of data, the control of algorithms, and the control of networks. Technology is thus to be treated not merely as an instrument in the hands of states, but as an active element that shapes actors' identities, interests, and modes of interaction. The perspective advanced here foregrounds an interdisciplinary and multilevel understanding that regards the insights of the realist, liberal, and constructivist traditions as complementary rather than opposed, and that brings together technical, legal, economic, and ethical dimensions within a single analysis.

Certain limitations of the study must also be stated plainly. The rapid evolution of digital technologies shortens the period over which the findings remain valid; in particular, the confidential nature of data on cyber capabilities, intelligence activities, and defense capacities narrows the scope of empirical examination. The study's focus on the great powers leaves the experiences of countries of the Global South relatively in the background; and its reliance on qualitative and interpretive methods limits quantitative generalizations and precise measurements of effect. Moreover, the analysis of these technically complex technologies in the language of the social sciences has inevitably required the simplification of certain details. These limitations make it necessary to interpret the findings with caution and to keep updating them through future studies.

Within this framework, several priorities stand out for policymakers. First, scheduling the migration of critical information systems to post-quantum encryption is a step that cannot be postponed where the protection of long-lived data is concerned; the international standards that have been published provide a ready foundation for this transition (NIST, 2024d). Second, the adoption of auditable common principles regarding the military and civilian use of artificial intelligence can be developed in alignment with existing international frameworks (OECD, 2019; High-Level Advisory Body on Artificial Intelligence, 2024). Third, strengthening the norms of responsible state behavior in the cyber domain and reducing the uncertainty surrounding attribution and retaliation are important for lowering the risk of unintended escalation (Schmitt, 2017). Fourth, there is a need to support multistakeholder governance mechanisms that render platforms' regulatory role in the public sphere accountable, that protect digital rights, and that limit the fragmentation of the internet (Bradford, 2023; DeNardis, 2020). These priorities are not independent of one another; they should be treated as parts of a coherent policy whole that constrains the disruptive potential of technology while enabling its beneficial use.

For future research, three orientations appear especially fruitful. The first is to move beyond the great-power-centered framework by examining the distinct trajectory of digital technologies in the Global South and by rendering the dimension of inequality visible. The second is to measure digital power more robustly through mixed methods that combine qualitative analyses with measurable indicators, thereby grounding theoretical inferences in empirical foundations. The third is to examine the compound effects produced jointly by technologies such as artificial intelligence, quantum computing, and blockchain in interaction with one another rather than separately. Pursuing these orientations calls for a research agenda based on inter-institutional collaboration that brings together computer science, law, economics, and political theory.

In conclusion, the transformation of international relations in the digital age makes a comprehensive review of the discipline's theoretical tools and methods imperative. Managing this transformation successfully depends on the coordinated development of academic knowledge, public policy, and institutional structures. It must not be forgotten that the consequences of technology are not predetermined, and that they will be shaped largely by the choices that societies and states make. For this reason, placing digital technologies in the service of an international order that produces peace, security, and prosperity is not merely a matter of technology; it will remain one of the most important shared political and ethical responsibilities of the twenty-first century.

References

1. Acemoglu, D., & Johnson, S. (2023). Power and progress: Our thousand-year struggle over technology and prosperity. PublicAffairs.
2. Agrawal, A., Gans, J., & Goldfarb, A. (2022). Power and prediction: The disruptive economics of artificial intelligence. Harvard Business Review Press.
3. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
4. Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141–165.
5. Arsenault, A. C., & Kreps, S. E. (2024). AI and international politics. In J. B. Bullock et al. (Eds.), The Oxford handbook of AI governance. Oxford University Press.
6. Bank for International Settlements. (2021). Central bank digital currencies: An opportunity for the monetary system. In BIS annual economic report 2021 (Chapter III, pp. 65–95). Bank for International Settlements.
7. Bjola, C., & Holmes, M. (Eds.). (2015). Digital diplomacy: Theory and practice. Routledge.
8. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40.
9. Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.
10. Braun, M., & Hummel, P. (2025). Is digital sovereignty normatively desirable? Information, Communication & Society, 28(10), 1721–1734.
11. Bremmer, I., & Suleyman, M. (2023). The AI power paradox: Can states learn to govern artificial intelligence before it is too late? Foreign Affairs, 102(5), 26–43.
12. Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton.

DOI: 10.5281/zenodo.21320691

13. Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.
14. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner.
15. Castells, M. (2015). Networks of outrage and hope: Social movements in the Internet age (2nd ed.). Polity.
16. Checkel, J. T. (1998). The constructivist turn in international relations theory. World Politics, 50(2), 324–348.
17. Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
18. Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
19. Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.
20. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE.
21. DeNardis, L. (2020). The Internet in everything: Freedom and security in a world with no off switch. Yale University Press.
22. Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods (2nd ed.). McGraw-Hill.
23. Ding, J. (2024). Technology and the rise of great powers: How diffusion shapes economic competition. Princeton University Press.
24. Drezner, D. W. (2019). Technological change and international relations. International Relations, 33(2), 286–303.
25. Dunn Cavelty, M., & Wenger, A. (2024). The evolution of cyberconflict studies. International Affairs, 100(6), 2317–2338.
26. European Commission. (2020). White paper on artificial intelligence: A European approach to excellence and trust. Publications Office of the European Union.
27. European Court of Human Rights. (2021). Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15), Grand Chamber judgment, 25 May 2021.
28. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
29. European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. Publications Office of the European Union.
30. European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. Publications Office of the European Union.
31. Fairclough, N. (2013). Critical discourse analysis: The critical study of language (2nd ed.). Routledge.
32. Farrell, H., & Newman, A. L. (2023). Underground empire: How America weaponized the world economy. Henry Holt.
33. Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. International Organization, 52(4), 887–917.
34. Flick, U. (2018). An introduction to qualitative research (6th ed.). SAGE.
35. Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. Oxford University Press.
36. Floridi, L. (2018). Soft ethics and the governance of the digital. Philosophy & Technology, 31(1), 1–8.
37. Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy.
38. Freedom House. (2024). Freedom on the net 2024: The struggle for trust online. Freedom House.
39. Fuchs, C. (2021). Social media: A critical introduction (3rd ed.). SAGE.
40. George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.
41. Gerring, J. (2007). Case study research: Principles and practices. Cambridge University Press.
42. Glasze, G., Cattaruzza, A., Douzet, F., et al. (2023). Contested spatialities of digital sovereignty. Geopolitics, 28(2), 919–958.
43. Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854–871.
44. Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network analysis for international relations. International Organization, 63(3), 559–592.
45. Hansen, L. (2006). Security as practice: Discourse analysis and the Bosnian war. Routledge.
46. High-Level Advisory Body on Artificial Intelligence. (2024). Governing AI for humanity: Final report. United Nations.
47. Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15(9), 1277–1288.
48. International Telecommunication Union. (2024). Measuring digital development: Facts and figures 2024. ITU.
49. Kello, L. (2017). The virtual weapon and international order. Yale University Press.
50. Keohane, R. O., & Nye, J. S., Jr. (2012). Power and interdependence (4th ed.). Longman.
51. Krippendorff, K. (2018). Content analysis: An introduction to its methodology (4th ed.). SAGE.
52. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038.
53. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE.
54. Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
55. Microsoft. (2024). Microsoft digital defense report 2024. Microsoft.
56. Microsoft. (2025). Microsoft digital defense report 2025. Microsoft.
57. Morozov, E. (2011). The net delusion: The dark side of internet freedom. PublicAffairs.
58. Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention. Chatham House.
59. Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? Journal of European Public Policy, 31(8), 2200–2225.

DOI: 10.5281/zenodo.21320691

60. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.
61. National Institute of Standards and Technology. (2024a). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). U.S. Department of Commerce.
62. National Institute of Standards and Technology. (2024b). Module-lattice-based digital signature standard (FIPS 204). U.S. Department of Commerce.
63. National Institute of Standards and Technology. (2024c). Stateless hash-based digital signature standard (FIPS 205). U.S. Department of Commerce.
64. National Institute of Standards and Technology. (2024d). Transition to post-quantum cryptography standards. U.S. Department of Commerce.
65. Ndzendze, B., & Marwala, T. (2023). Artificial intelligence and international relations theories. Palgrave Macmillan.
66. Nye, J. S., Jr. (2011). The future of power. PublicAffairs.
67. O'Hara, K., & Hall, W. (2021). Four internets: Data, geopolitics, and the governance of cyberspace. Oxford University Press.
68. Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence. OECD Publishing.
69. Organisation for Economic Co-operation and Development. (2024). OECD digital economy outlook 2024 (Vol. 1). OECD Publishing.
70. Organisation for Economic Co-operation and Development. (2025). A quantum technologies policy primer. OECD Publishing.
71. Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). SAGE.
72. Rid, T. (2013). Cyber war will not take place. Oxford University Press.
73. Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. Ethics and Information Technology.
74. Rodríguez, A. G. (2025). Cybersecurity implications of quantum computing and its combined use with artificial intelligence. UNISCI Journal, 67, 137–162.
75. Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton.
76. Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
77. Schwab, K. (2016). The fourth industrial revolution. World Economic Forum.
78. Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
79. Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), 63–75.
80. Singer, P. W., & Brooking, E. T. (2018). LikeWar: The weaponization of social media. Houghton Mifflin Harcourt.
81. Smith, M. R., & Marx, L. (Eds.). (1994). Does technology drive history? The dilemma of technological determinism. MIT Press.
82. Srivastava, S., & Bullock, J. B. (2024). AI, global governance, and digital sovereignty.
83. Stanford Institute for Human-Centered Artificial Intelligence. (2024). Artificial intelligence index report 2024. Stanford University.
84. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.
85. United Nations. (2021). Our common agenda: Report of the Secretary-General. United Nations.
86. United Nations Human Rights Council. (2012). The promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/20/8). United Nations.
87. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151.
88. Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications. Cambridge University Press.
89. Wendt, A. (1999). Social theory of international politics. Cambridge University Press.
90. West, D. M. (2018). The future of work: Robots, AI, and automation. Brookings Institution Press.
91. World Bank. (2022). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. World Bank.
92. World Economic Forum. (2025). Global cybersecurity outlook 2025. World Economic Forum.
93. World Economic Forum. (2026). Global cybersecurity outlook 2026. World Economic Forum.
94. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE.
95. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

DOI: 10.5281/zenodo.21320691