Techno Feudalism and the New Global Power Struggle: Echoes of a Digital Cold War

Elgun Taghizade[1], Elchin Ahmadov[2]

[1]Faculty of International Relations and Economics, Department of Diplomacy and Modern Integration Processes, Baku State University, Baku, Azerbaijan - PhD

[2]Faculty of Political Sciences and Journalism, Maria Curie-Skłodowska University, Lublin, Poland- Master's degree

DOI: https://dx.doi.org/10.47772/IJRISS.2025.9020093

Received: 18 January 2025; Accepted: 31 January 2025; Published: 04 March 2025

ABSTRACT

The 21st century has been one of great change in the global economic, political, and social landscapes, thanks to rapid technological advances—reshaping them all into a new techno-feudal order dominated by Big Tech. This paper presents an analysis techno-feudalism and the upcoming Cold War that is digital, where corporations' control over digital infrastructure and data is reminiscent of medieval feudalism. These "digital lords" extend influence far beyond markets, challenging state sovereignty and transforming international relations.

The paper focuses on the rapidly growing US-China rivalry in artificial intelligence, cybersecurity, big data, and 5G technology. It flags how these technologies are being weaponized against cyberattacks and economic disruptions, reconfiguring governance and global security. In contrast to the decentralized strategies of the US Big Tech, China's centralized use of AI, as represented by its Social Credit System, has brought about fast changes in its technological development while affecting social norms and economic arrangements.

The study adopted a mixed-method approach that includes qualitative and quantitative analyses, as well as case studies and the Delphi technique. The major findings explain how digital monopolies stifle competition, how cyber warfare could destabilize critical infrastructure, and to what extent Big Tech is increasingly affecting governmental policies and societal norms. Examples include ransomware attacks like the Colonial Pipeline incident and the WannaCry malware attack, pointing out vulnerabilities of the global digital infrastructure and associated economic consequences.

Emphasis is placed on the need for immediate international regulatory frameworks to address the ethical, economic, and security concerns brought about by techno-feudalism and the Digital Cold War. This article encourages cooperation in the aspects of risk reduction, promotion of equitable technological development, and reinforcement of security measures worldwide. This paper serves to significantly expand one's knowledge of the power dynamics at play in the digital age and their consequences for relations among nations.

Key Words: Techno-Feudalism, Digital Cold War, Digital Monopolies, Artificial Intelligence, International security

INTRODUCTION

In the contemporary digital era, monopolies have evolved beyond traditional industries to dominate the digital space, exerting unprecedented influence over economies, societies, and even political systems. These digital monopolies, often referred to as "techno-feudal lords," control vast amounts of data, digital infrastructure, and online platforms, shaping economic structures and global governance (Taghizade & Ahmadov, 2024, p. 5). A digital monopoly is characterized by a company's exclusive control over a particular market, service, or technological ecosystem. Companies such as Google, Amazon, Meta, and Tencent hold monopolistic positions in online advertising, e-commerce, and social media, respectively. For example, Google's market share in

search engines stood at 91.88% as of June 2022, illustrating its overwhelming dominance (Kinsta, 2022). This concentration of power is further reinforced by proprietary algorithms, which allow digital giants to shape public perception and influence political outcomes. Google's advertising monopoly, for instance, has led to lawsuits by the U.S. Department of Justice, accusing the company of engaging in anti-competitive behavior by acquiring competitors and coercing publishers to use its advertising tools (Robertson, 2024). Political theorist Yanis Varoufakis has coined the term "techno-feudalism" to describe a system where digital monopolies function like medieval lords, controlling economic activities and extracting digital rents from users and smaller businesses. Unlike traditional capitalism, where competition fuels innovation, techno-feudalism consolidates control in the hands of a few digital elites (Varoufakis, 2023).

Through a concept known as “platform sovereignty,” companies like Google, Amazon, and Meta establish their own governance models, setting rules for digital labor, content moderation, and data usage without state oversight. This leads to the privatization of governance, challenging the authority of nation-states (Wineberg, 2025). The monopolistic control exercised by tech giants has far-reaching economic consequences. These corporations often stifle competition by acquiring emerging rivals or making it financially unviable for competitors to sustain their businesses. The monopolization of digital infrastructure leads to increased advertising costs, suppression of innovation, and reduced consumer choices (Dobusch & Kreissl, 2024). Furthermore, digital monopolies have blurred the boundaries between corporate influence and political decision-making. Companies such as Tencent, through platforms like WeChat, not only control digital interactions but also share user data with state authorities, reinforcing state surveillance capabilities. This intersection of private control and government oversight is particularly evident in China, where Alibaba and Tencent serve as de facto arms of the state, integrating AI and big data into governance structures (Muhleisen, 2018,).

A critical manifestation of digital monopolies is their role in the so-called "Digital Cold War," primarily involving the U.S. and China. This competition extends beyond traditional market dominance into areas such as artificial intelligence, cybersecurity, and big data. While American companies like Google and Amazon operate under a market-driven model, their Chinese counterparts, including Baidu, Alibaba, and Tencent, operate in close coordination with the state (Biddle, 2015). China’s Social Credit System exemplifies how digital monopolies can be leveraged for national governance. By integrating vast amounts of citizen data, the system assigns scores that determine social privileges, reinforcing state control through technology. This model is in stark contrast to the decentralized approach seen in the West, where private corporations wield significant influence but remain relatively independent of direct government intervention. The unchecked expansion of digital monopolies raises urgent questions about the need for international regulatory frameworks. Given their economic and political power, these companies require stringent antitrust regulations and greater public accountability. The August 2024 ruling by Judge Amit Mehta, which declared Google a monopolist in violation of U.S. antitrust laws, marks a significant step in this direction (Robertson, 2024). At the international level, organizations such as the United Nations and the World Trade Organization must develop mechanisms to regulate the influence of digital monopolies. This includes ensuring data privacy protections, preventing anti-competitive mergers, and establishing digital taxation policies to curb the economic dominance of tech giants (Bremmer, 2021). Digital monopolies have become a defining feature of the modern global economy, shaping political discourse, economic structures, and international power dynamics. The emergence of techno-feudalism, characterized by the unchecked dominance of tech giants, calls for urgent regulatory reforms to prevent further economic stratification and the erosion of state sovereignty. Without such interventions, the world risks shifting from traditional capitalist competition to a new form of digital aristocracy, where control over data and digital infrastructure determines global influence.

One of the most pressing concerns surrounding digital monopolies is their influence on governance. Tech giants increasingly assume roles traditionally held by governments, from controlling information flows to setting labor standards. The concept of "platform sovereignty" describes how these corporations create their own legal and economic ecosystems, often beyond the reach of national regulations (Wineberg, 2025). This erodes state power and creates governance gaps that undermine regulatory effectiveness. Moreover, the "Digital Cold War" between the United States and China exemplifies the geopolitical struggle over technological dominance. The U.S. and its allies face growing challenges in regulating Chinese tech companies such as Tencent and Alibaba, which integrate AI-driven surveillance into their business models (Biddle, 2015).

Meanwhile, China's Social Credit System, which relies on data collected by private tech firms, represents a case of corporate-state collaboration to enforce social compliance (Muhleisen, 2018). These developments highlight how digital monopolies blur the lines between private and state power, complicating global governance. Digital monopolies shape societal structures by influencing public discourse, labor markets, and privacy standards. Google and Meta control vast amounts of online information, using algorithmic filtering to curate search results and news feeds, potentially shaping political narratives (Jedlickova, 2024). This creates concerns about election interference and the suppression of dissenting voices. The rise of the gig economy, dominated by companies like Amazon and Uber, further exacerbates social inequalities. These platforms rely on precarious labor models that strip workers of traditional employment protections, leaving them vulnerable to exploitation (Dobusch & Kreissl, 2024). The lack of regulatory oversight in this sector allows digital monopolies to dictate terms that favor corporate interests over worker rights.

Another major societal concern is the erosion of privacy. The extensive collection of user data by digital monopolies raises ethical questions regarding surveillance capitalism. Tech giants monetize personal data through targeted advertising and predictive analytics, reducing consumer autonomy while increasing corporate profits (Zuboff, 2019). Such practices not only compromise privacy but also reinforce systemic biases in AI-driven decision-making.

The monopolistic behavior of tech giants significantly impacts global economic structures. Digital monopolies stifle competition by acquiring potential rivals or engaging in anti-competitive practices. Google's control over the online advertising market has led to lawsuits alleging market manipulation and unfair business practices (Jedlickova, 2024). Similarly, Amazon's aggressive pricing strategies force smaller retailers out of business, consolidating market power within a single entity. Cybersecurity vulnerabilities further threaten economic stability. The reliance on digital infrastructure has exposed financial institutions and governments to cyberattacks, with incidents like the Colonial Pipeline ransomware attack demonstrating the fragility of interconnected economies (Feingold & Wood, 2024). The increasing frequency of cyber warfare underscores the need for stronger regulatory frameworks to mitigate economic risks posed by digital monopolies. Tech corporations wield immense political influence through lobbying efforts and policy interventions. Companies such as Amazon and Google invest heavily in political lobbying to shape regulations in their favor, ensuring minimal government intervention in their operations (Swanson, 2022). This undermines democratic processes by allowing corporate interests to override public policy concerns. The political weaponization of digital platforms is another alarming trend. Disinformation campaigns, facilitated by algorithmic manipulation, have been used to influence elections and destabilize political institutions. The role of social media in the spread of fake news and extremist ideologies highlights the dangers of unchecked digital monopolies in democratic societies (Bremmer, 2021). Moreover, digital monopolies play a critical role in cyber warfare. State-sponsored cyberattacks targeting critical infrastructure have become a central strategy in geopolitical conflicts. The militarization of cyberspace demonstrates how digital monopolies, either willingly or through coercion, become key players in international security (Mueller, 2013). Digital monopolies present unprecedented challenges to governance, society, the economy, and politics. Their unchecked expansion threatens democratic institutions, exacerbates economic inequality, and undermines national sovereignty. Addressing these issues requires a coordinated international effort to establish regulatory frameworks that promote fair competition, protect consumer rights, and safeguard democratic values. Without such measures, digital monopolies will continue to reshape global power dynamics in ways that prioritize corporate dominance over public interest.

Reseach gap - the advancement of technology over the years has begun to signal the emergence of a new world system. Since technology companies now possess the capacity to influence contemporary politics, a new concept has emerged technofeudalism. The literature on this topic touches on the economic aspects of techno-feudalism but lacks a deep exploration of its political and social consequences, such as the erosion of democratic institutions, shifts in governance, and implications for individual freedoms. However, this article delved into the political and social dimensions of techno-feudalism, analyzing how digital monopolies influence governance structures, public policies, and personal liberties. It also examined the implications for political participation and public trust in democratic systems. Technofeudalism critiques the rise of techno-feudalism, it offers limited suggestions for addressing the challenges posed by this new power structure. But, this article explored potential solutions and alternatives, discussing how societies, governments, and international organizations can resist the rise of techno-feudalism. It considered regulatory frameworks, and

technological innovations as possible countermeasures. The literature on this topic discusses the rise of techno-feudalism in the context of digital monopolies but does not explore in depth how emerging technologies (for example AI, blockchain, automation) specifically contribute to reinforcing techno-feudal power dynamics. This article addressed this gap by examining the role of emerging technologies in reinforcing techno-feudalism. We analyzed how AI, automation, and blockchain technologies might further concentrate power, wealth, and control in the hands of a few, deepening the divide between digital elites and the general population.

Literature Review Since this is a new topic, it is scarce in the literature, and this article has been developed based on the existing literature and our ideas. The key points on this issue have been highlighted. For example, Varoufakis (2023), in Technofeudalism: What Killed Capitalism, presents a clear argument that capitalism has not only changed but has been effectively replaced by a system where digital platforms function as feudal estates. He argues that tech giants like Google, Amazon, and Facebook operate as digital landlords, extracting economic rent from users and businesses that depend on their infrastructure. Unlike traditional capitalists who profit through competitive production, these digital overlords accumulate wealth by controlling access to data, platforms, and digital services, creating a dependency akin to medieval feudalism. The evolution of human civilization has been characterized by waves of technological innovation, as described by Alvin Toffler in his seminal work The Third Wave (1980). Toffler identified three revolutionary waves: agricultural, industrial, and informational that have reshaped societies. Today, we stand at the precipice of a fourth wave, driven by advancements in AI and other emerging technologies. This new era, often referred to as the Fourth Industrial Revolution, is "fundamentally changing the way we live, work, and relate to one another," as noted by Klaus Schwab (2016, p. 2). It already means that with the advancement of technology, a new system is forming, and those who own this technology will be the ones influencing the global system. Building on that concept, French economist Cédric Durand (2020) adds that techno-feudalism is a system through which Big Tech cements its economic dominance using monopolistic practices and control over critical digital infrastructures. These companies thus create "digital dependencies" that make it impossible for societies to function without their platforms, further cementing their power over individuals and states. The rise of techno-feudalism overlaps with a "Digital Cold War," an aggressive competition between states, namely the U.S. and China, for technological primacy. Unlike the 20th-century Cold War, this conflict is centered around issues of AI, big data, and cybersecurity. Scholars like Shoshana Zuboff (2019) highlight how surveillance capitalism rooted in the extraction and manipulation of user data—intensifies this global competition. The struggle extends beyond states, with tech corporations becoming pivotal actors in international relations, influencing sovereignty and security. These developments signal a profound shift in global power dynamics, where traditional state sovereignty is challenged by corporate dominance. Techno-feudalism is the rewriting not only of economic systems but also of social and political landscapes, which need new governance frameworks to deal with the ethical, economic, and geopolitical problems caused by digital monopolies. These writings underline the importance of considering and working out the profound consequences of techno-feudalism in the reformation of economic systems, political structures, and power dynamics in the world.

This article examines techno-monopolies through the lens of Neofeudalism Theory in Digital Capitalism, which frames the dominance of tech giants as a modern form of feudal power. Unlike traditional capitalism, where competition drives innovation, techno-feudalism reduces control in the hands of a few digital elites, limiting market dynamism and user autonomy (Wineberg.D., 2025). Through this perspective, the techno-monopoly problem is not only an issue of market concentration but a fundamental shift in governance, where corporations function as quasi-sovereign entities, dictating economic, social, and even political norms. Algorithmic control and data extraction serve as digital rent-seeking mechanisms, reinforcing economic stratification and deepening societal dependence on platform-driven ecosystems. By problematizing techno-monopolies as digital fiefdoms, this approach highlights the erosion of democratic oversight, the growing precarity of digital labor, and the increasing difficulty of challenging corporate hegemony in the global order. The techno-monopoly problem is analyzed through the lens of Platform Sovereignty, where digital platforms like Google, Amazon, and Meta function as quasi-sovereign entities, operating beyond traditional state control. These platforms establish rules, control digital infrastructure, and influence economic and political life. This lens highlights how techno-monopolies not only dominate markets but also privatize governance, regulating digital labor and public discourse. The result is a shift in power from states to corporations, undermining state sovereignty and creating a new form of corporate hegemony that challenges democratic oversight.

Methodology - This study employs a mixed-methods approach, integrating both quantitative and qualitative research methods to analyze techno-feudalism. The research is conducted within an objective and interpretive framework, combining objectivism and subjectivism in its ontological approach, while applying rationalism and empiricism for data interpretation. For data collection, the study utilizes both quantitative and qualitative methods. Cross-sectional surveys were conducted among university students and faculty to gather empirical data, and the Delphi method was employed to obtain expert consensus on future developments. Case studies were incorporated for context-based analysis, while document analysis was performed on official and historical records. Additionally, public interviews with students and teachers provided qualitative insights, and observational, descriptive, and analytical approaches were used to interpret the collected data. To ensure data accuracy and reliability, a triangulation method was applied, verifying sources across multiple datasets. Comparative analysis was conducted to cross-check findings, and synthesized data from various sources was integrated to enhance validity. For data analysis, the study employed inductive and deductive reasoning to develop arguments, while comparative analysis was used to identify patterns and relationships. The Delphi method also facilitated predictive analysis for assessing future trends. This structured methodological framework ensures a comprehensive and rigorous examination of techno-feudalism, combining empirical research with analytical depth.

Research questions :

1. How do tech-monopolies shape competition, innovation and restructure global power dynamics?
2. To what extent do technology companies influence the decision-making processes of governments, and in what areas is this influence most evident?
3. How does the Digital Cold War between the United States and China impact global governance and international security?

Hypothesis:

1. There is a correlation between tech monopolies and their influence on international governance.
2. Tech companies dominate certain sectors but do not control entire markets.
3. The economic and informational power of tech companies influences global policies and market dynamics.
4. Tech monopolies impact government decisions on digital infrastructure, economic policy, and data privacy.
5. The Digital Cold War between the U.S. and China increases global tensions and weakens international cooperation.

New perspectives on the digital cold war

The term "Digital Cold War" originates from the classic "Cold War" and describes the competition between states and major tech companies over technology, cybersecurity, and information control. This struggle, particularly between the US and China, revolves around digital infrastructure, cyber espionage, artificial intelligence, and Big Data. The classic Cold War was the political, economic, military, and ideological competition between the United States and the Soviet Union between 1947 and 1991, after the Second World War. Over time, the security dilemma and aspiration toward hegemony forced both sides. The important point here is that in the attainment of mutual superiority through nuclear deterrence, espionage, propaganda, and regional conflicts, both sides fought without a confrontation. The fact that technological development is one of the main criteria of power in the modern era leads to the current processes being more specifically referred to as a kind of "Digital Cold War". Many parts of our article can be quoted to support this factor. In other words, only 2 of the world's 10 most valuable companies are not technology companies (6th Saudi Aramco, 9th Berkshire Hathaway). The remaining 80% are either tech companies or companies dealing with the field of

technology. (1. Apple, 2. Nvidia, 3. Microsoft, 4. Amazon, 5. Alphabet, 7. Meta Platforms, 8. TSMC, and 10. Broadcom.) (Companies Market Cap, 2024) As we can see from this small example, the main battlefield of modern times is the technological one. To make this process clearer, it is necessary to underline the main differences between today's Digital Cold War and the classical Cold War. So it can be divided into 3 main headings:

1. Battlefield and Tools: While military power and nuclear threats are in the foreground of the Classical Cold War, areas like cyber security, artificial intelligence, big data, and communication technologies are strategically significant in the Digital Cold War. Here, issues related to the control of digital infrastructures and data security come to the fore.

2. New Actors: States used to be the main actors during the classic Cold War. Today, big technology companies, such as Google, Amazon, Huawei, and Microsoft, have emerged as important actors. Their influence over governments, global power, and their role in the economy make them part and parcel of the digital war.

3. Global Integration: Due to globalization and digitalization, there has been an intensification of economic and technological relations and risen interdependence between nations. The modern cold war has thus been much more complex, and direct confrontation between states could shake up the world economy altogether.

The Digital Cold War affects global security, privacy, and economic stability. Cyberattacks deteriorate trust between states, heighten national security risks, and disrupt economies. AI-driven warfare, cyber espionage, and digital monopolies fuel political and ethical debates. Historically, Cold War conflicts involved proxy wars, nuclear arms races, and ideological struggles. Now, cyber intelligence, economic espionage, and Big Data manipulation define geopolitical competition. The rise of cyber groups, both state and non-state actors adds complexity to international relations.

At the same time, it has to be mentioned that the very "digitalization process" has a huge impact on nearly every side of people's lives. This impact causes humans to create new weapons and new defense methods. For example, before the digitization process, states used to store and encrypt confidential information on paper and similar methods. Obtaining this data was very difficult and time-consuming. Nowadays, dozens of new types of "Data Breaches" are taking place due to cyber-attacks. For instance, the Yahoo Data Breach affected 3 billion accounts. Another example is Aadhaar, where the identity and biometric data of 1.1 billion Indian citizens leaked.

This leads us to our conclusion that no matter how little data space is occupied during digitization, it brings negative and positive aspects. Again, a lot of new problems have emerged such as ethical issues, the need to introduce and develop new norms to international legal norms, the vulnerability of traditional nation-states' attacks in the digital age, and the impact on national security(Hill & Swinhoe, 2022)

The Economic Disruption and Financial Cyber Attacks in the Era of Digitalization

Another sphere of influence of the digital cold war in contemporary times is manifested directly in economic disruption. Economic disruption thus refers to deliberate actions to disrupt or undermine the economic system, stability, and growth dynamics of a country or region. That activity has been carried out for economic, political, or military motives. It is very evident in modern-day scenarios such as digital warfare, Cold War tactics, and financial assaults. It also causes adverse effects on economic data through changes in the perception of the economic system and spreading gloomy pictures, etc. As a result, businesses fail, unemployment surges, the financial system melts down, interest rates climb and social disasters emerge.

Today, the digitalization of economic systems also opens the door to digital attacks. In other words, as in the IMF report, today, global financial stability is in danger because of cyber-attacks. There is no guarantee that states and organizations will not attack the vulnerabilities brought about by the digitalization of the system, whereby this process is one of the elements of the digital cold war. Considering that in 2017, the total amount of money in the world was 90.4 trillion dollars and 92% of it was Non-Physical funds. At the same time, with

reference to the Harvard Business Review of 2021, we may state that over 97% of all existing money circulates in online transactions. Of course, along with the data we mentioned, cyber-attacks have been carried out in that way. Some examples of Financial Data Breaches (Feingold, S., Wood, J., & World Economic Forum,2024):

1. First American Financial Corp Data Breach: The real estate transactions of over 885 million people were exposed in a design disaster on the web in May 2019. Here, first and last names, e-mail addresses, phone numbers of closing agents and buyers data were exposed. Cyber crimes that people armed with this information can leverage range from identity theft to Ransomware attacks, Malware injections, and malicious program infections (Kost, E,2022).

2. Equifax Data Breach (EDB): EDB, which we mentioned above, also belongs to financial cyber-attacks. More than 147 million people's data were compromised, including first and last names, birth dates, social security numbers, driver's license numbers, and credit card numbers used in financial cyber-attacks. Because of this process, Equifax was fined around 700 million U.S. dollars (Kost, E,2022).

3. Heartland Payment Systems Data Breach: In another financial cyber attack, in January 2008, Russian hackers conducted an SQL injection attack that pierced the Heartland Payment Systems' network and compromised credit card information. Within roughly 6 months, hackers bypassed antivirus protections and installed "sniffer" software that uncovered the credit card numbers of 130 million users. The attack was perpetrated by Albert Gonzalez and two of his friends; Gonzalez received a 20-year prison sentence. The company later beefed up its cybersecurity and introduced a leakage guarantee for customers. A few months later, however, an attack on its human resources department led to the theft of 11 computers and the leak of personal information of about 2,200 people. An incident like this really puts into perspective that mere compliance standards are not enough. Additional security measures, physical protection, and third-party risk management all need to be in place (Kost, E,2022).

In this regard, one may note a number of financial cyber-attacks, each of which resulted in the theft of millions of people's financial data as a result of the attacks. Briefly: Capital One Data Breach (Impact: 100 million credit card applications), JPMorgan Chase Data Breach (Impact: 83 million accounts), Experian (Impact: 24 million customers), Block (Impact: 8.2 million employees), Desjardins Group (Impact: 4.2 million customers) and others.

According to the above information, in this digital Cold War era, states and organizations tried to weaken the adversary side in the digital environment by using cyber attacks, including disruption of economic systems, financial attacks, and personal data leaks. This digitalization of infrastructure, the fact that monetary transactions are mostly conducted online, and the global networking of states' economic systems create a fertile ground for the success of cyberattacks. It, therefore, brings about huge financial losses, companies going bankrupt, a rise in unemployment, and a threat to economic stability.

These attacks, which exploit the loopholes of cyber-criminality, prove that in this new era, genocidal warfare continues in the digital arena. As in the case of Financial Data Breaches, mass information leaks resulting in the loss of information of millions of people pose serious risks to financial institutions and economic systems. This situation clearly shows that digital warfare is being continued on the basis of economic positions and that global economic stability is always under threat, and throws light on what will take place in the further development phase of the digital genocide warfare.

What is Techno-Feudalism?

Techno-Feudalism is a concept that has gained significant attention in recent years, particularly in the context of the digital economy and the rise of tech giants. Techno-Feudalism is a socio-economic theory suggesting that capitalism is being replaced by a new system dominated by Big Tech corporations. The term draws an analogy to medieval feudalism, where power was concentrated in the hands of a few lords who controlled land and resources. Today, instead of land, technology companies like Amazon, Google, Facebook, and others hold control over vast digital infrastructures, data, and online platforms, positioning themselves as the new "lords" of the digital realm. The direct influence of these corporations on many states, their power over many states, and their overall supranational power, leads us to call them the “Feudals” of the modern era. To give a small

example, Apple's market capitalization (3.4 trillion dollars) compared to the countries of the world shows its valuation power in the financial markets rather than its production activity, and if Apple were a country, it would rank 5th in the world GDP ranking. With this market capitalization, it would rank second behind Germany and Japan. At the same time, Apple's annual revenue (around $400 billion) outstrips the GDP of many countries. This revenue is higher than the GDP of Finland or Portugal, ranking 39th in the GDP ranking (Worldometer, 2023).

Yanis Varoufakis refers to techno-feudalism as a socioeconomic system that has emerged from capitalism but represents a radical change in the power relationship. What he called "cloud capital" refers to this system, depending on capital grounded in technology and digital infrastructure rather than traditional means of production like machines or land. The very nature of techno-feudalism is that the distribution of wealth and power no longer rests with the main profiteers of the industrial output and the competition of markets. It rests, rather, with those who control the digital platforms and the behavior-modifying technology associated with them. The analogy to the shift from feudalism to capitalism and now to techno-feudalism is an important one. In feudalism, the repository of wealth and power depended on land ownership and ground rent. Under capitalism, power passed to the owners of machinery and manufacturers of goods, as profit became the dominant accumulative form, displacing rent. Under techno-feudalism, cloud capital functions much the same way as digital "land" in creating virtual domains or "digital fiefdoms," such as Amazon.com. In those fiefdoms, platform owners not only extract value from the consumers but also the producers by imposing fees, which are similar to the ground rent of feudal times(How To Academy.2024). Simultaneously, French economist Cédric Durand, in his 2020 book Technoféodalisme: Critique de l'Économie Numérique, argues that Big Tech companies have created monopolies by using advanced methods to extract and control data. These platforms become so essential to modern life—much like utilities such as electricity or telecoms—that societies become dependent on them, making it nearly impossible to function without their services. This dependence gives tech companies immense power, much like feudal lords once held over land and resources (Durand, 2020).

Such a question may arise—"How is Techno-Feudalism different from Capitalism? "- It avoids traditional markets and mechanisms of profit. In the classical sense, Amazon, Google, and Uber are not markets because they exert control over the entire transaction process through algorithms. Algorithms change behavior in such a way that both predicting and influencing consumers' preferences sidelines the classic capitalist competition that once characterized market-driven economies. Varoufakis believes this is the end of capitalism and the beginning of a new system using technology to extract cloud rent, not profit, as the main source of wealth accumulation.

Furthermore, Varoufakis suggests that this transformation has deep global implications. The rivalry between the U.S. and China, both dominant in cloud capital, could lead to geopolitical tensions, potentially manifesting in conflicts akin to a new Cold War. Thus, techno-feudalism not only changes economic structures but also reshapes international relations and the global power balance (Barbora Jedlickova, 2024).

Moreover, Varoufakis' concept of techno-feudalism represents a multi-layered paradigm that affects not only economic transformations but also social and political structures. In this new system, the use of digital platforms not only as economic power but also as a means of social control allows individuals not only to direct their consumption behavior but also to create hegemony over public and private spheres. In this context, Varoufakis' techno-feudalism can be considered as an "economy of management and control" that goes beyond classical capitalism. Such societal impacts of digital platforms suggest that the new power dynamics that come with technology should be considered in a broader international security and geopolitical context. In particular, the increasing information sovereignty of states and big tech companies could lead to the empowerment of non-state actors and the emergence of national security threats shaped by new digital tools.

The Rise of Techno-Feudalism

In recent years, there has been a growing debate about the sustainability of capitalism as a dominant global economic system. Having considered the mounting evidence of market distortions and inequalities, many economists and theorists have begun to explore whether capitalism is evolving into something fundamentally

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

different. One of these theories that has gained currency is the idea of 'techno-feudalism,' a term Yanis Varoufakis uses to describe a new socioeconomic order that, while emerging from capitalism, represents a radical reorganization in the structuring of wealth and power for the digital age. As it seems that traditional market mechanisms are becoming increasingly detached from real-world economic outcomes, it becomes very important to question whether capitalism as we know it is giving way to a new economic system—one that will fundamentally change the relationship between labor, capital, and technology. This is how capitalism is coming to an end: not with a revolutionary explosion, but with an evolutionary groan. Just as feudalism was slowly undermined until one day human relations were largely shaped by the market and feudalism was swept away, so today capitalism is giving way to a new economic style: techno-feudalism. The signs have been there for some time. Bond and equity prices, which should be moving in sharply opposite directions, have been rising violently together, always moving in the same direction, even if they occasionally fall. Similarly, the cost of capital, which should be falling with volatility, is rising as future returns become more uncertain. Perhaps the clearest sign that something serious was going on came in 2019. On that day, the UK's national income fell by more than 20 percent in the first seven months of 2020, exceeding even the most pessimistic forecasts. Just a few minutes later, the London Stock Exchange gained more than 2 percent. Nothing like this had ever happened before. Finance was completely decoupled from the real economy (Varoufakis, Y, 2020). But do these unprecedented events really mean that we no longer live under capitalism? Capitalism has been transformed at least twice since the late nineteenth century. Its first major transformation from competitive to oligopoly took place with the second industrial revolution, when electromagnetism brought together vast networks of corporations and the mega-banks needed to finance them. Adam Smith's baker, brewer and butcher were replaced by Ford, Edison and Krupp as the main driving forces of history. The cycle of mega-debts and mega-returns finally led to the crash of 1929, the New Deal program and the Bretton Woods system, which provided a rare period of stability after the Second World War with all its restrictions on finance.

The end of Bretton Woods in 1971 led to the second transformation of capitalism. As America's growing trade deficit became the world's largest supplier of aggregate demand - absorbing the net exports of Germany, Japan and then China - the US accelerated capitalism's most energetic phase of globalization, and German, Japanese and then Chinese profits flowed back to Wall Street to finance it all. But in order to play their part, Wall Street workers demanded to be freed from the constraints of the New Deal and Bretton Woods. With deregulation, oligopolistic capitalism became financialized capitalism. Just as Smith's baker, brewer and butcher were replaced by Ford, Edison and Krupp, the new heroes of capitalism are now Goldman Sachs, JP Morgan and Lehman Brothers. While these radical transformations have had serious consequences (the Great Depression, the Second World War, the Great Recession and the Long Recession after 2009), they have not eliminated the fundamental characteristic of capitalism: a system driven by personal profit and rent achieved through a market. After 2008, everything changed. After the central banks of the G7 countries came together in April 2009 to use their money printing capacity to re-float global finance, deep instability set in. Today, the global economy is powered not by private profit, but by the continuous money creation of central banks. Meanwhile, value creation has increasingly shifted away from markets to digital platforms such as Facebook and Amazon, which no longer operate like oligopolistic firms but rather like private fiefdoms or estates. The fact that central bank balance sheets, not profits, sustain the economic system explains what happened on August 12, 2020. Upon hearing the tragic news, financiers thought to themselves: “Great! The panicked Bank of England will print more pounds, which will flow to us. Now is the time to buy shares!” Across the West, central banks are printing money, financiers are lending it to companies, which are buying back their shares. Meanwhile, digital platforms have replaced markets as a means of accumulating personal wealth. For the first time in history, everyone is producing for free for the capital stock of large corporations. That's what it means to upload something to Facebook or connect to Google Maps to go somewhere. Of course, this does not mean that traditional capitalist sectors have disappeared. In the early nineteenth century, many feudal relations remained intact, but capitalist relations were beginning to dominate. Today, capitalist relations remain, but techno-feudalism relations have begun to overtake them. Although capitalism seems to be approaching its end with a whimper, it could also be followed by an explosion. If those suffering from techno-feudal exploitation and mind-boggling inequality can find a common voice, it is bound to boom (Conversation, 2022).

The Role of Technology in Shaping Global Power Structures

In the current century, technology has emerged as the most important factor that dictates the balance of power

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

around the world. Unlike in the past centuries, where relations between countries were influenced majorly by either military or economic strength, power today is fast shifting towards control over the digital medium, management of the available information, and technology such as artificial intelligence among others. Thus, in a way, these corporations are becoming the new states, hence transcending the traditional influence of states. Major technological companies, be it Google, Amazon, or Meta, have in their possession powers that are colossal, primarily because of their control over data. Having billions of users globally, these platforms have a direct impact on the flow of information, shaping public discourse, consumer behavior, and even political decisions. Others have even gone so far as to term this shift "techno-feudalism" because of the tech companies' similarity to feudal lords who rule over vast digital territories and command incredible resources. According to political theorist Yanis Varoufakis, in the techno-feudal world, traditional capitalist rules are disrupted, with tech giants becoming "rent-seeking" entities that extract value from the users and smaller businesses dependent on their platforms (How To Academy, 2024) .

Google is uniquely privileged in terms of manipulating information exposed to a global audience. It uses mostly proprietary and unclear algorithms, favoring certain kinds of information over others. This capacity can influence the outcomes of political campaigns, consolidate stereotypes, and shape consumer behavior and economic dynamics.

For instance, former U.S. President Donald J. Trump has alleged that : "It has been determined that Google has illegally used a system of only revealing and displaying bad stories about Donald J. Trump, some made up for this purpose while, at the same time, only revealing good stories about" Democratic presidential candidate Kamala Harris.This is an illegal activity, and hopefully the Justice Department will criminally prosecute them for this blatant interference of elections, if not, and subject to the laws of our country, I will request their prosecution, at the maximum levels, when I win the election, and become president of the United States.

But apart from public perception, Google holds an extraordinary 'soft power' in the sense of its ability to shape cultural and political processes without the use of coercive measures. This is much more than just an issue of content selection. Structurally, Google has dominated the digital economy, especially by holding a monopoly over the online advertising market. The U.S. Department of Justice has filed a lawsuit accusing Google of maintaining a monopoly in this sector. According to the charges, Google achieved its market dominance by acquiring competitors and coercing publishers into using its advertising tools in an effort to gain control over the whole digital advertising ecosystem.

A monopoly is defined as the exclusive possession or control of the supply or trade in a commodity or service. The allegations suggest that Google’s monopolistic practices have driven out competitors, increased advertising costs, stifled innovation, and ultimately harmed both publishers and consumers. If proven, these practices would indicate that Google unlawfully used its market dominance to eliminate competition, further strengthening its control over the flow of global information and the broader digital economy.

As a result, it is important to note that on August 5, 2024, Judge Amit Mehta issued a critical ruling regarding Google’s market practices. He stated, “the court reaches the following conclusion: Google is a monopolist, and it has acted as one to maintain its monopoly. It has violated Section 2 of the Sherman Act.” (Robertson, A, 2024)This ruling underscores the legal recognition of Google's monopolistic behavior, further solidifying the claims of unfair competition and market control that have been discussed. By affirming that Google violated antitrust laws, this judgment sets a significant precedent, reinforcing the broader argument that large technology companies can exert disproportionate influence over both economic systems and democratic processes.The new race for world domination is now underway, with AI and Big Data forming the most influential weapons. States and organizations that hold the cutting-edge technologies of AI have in their possession the means to wield economic and political forces through automation, predictive analytics, and different forms of e-surveillance. The advanced digital engineering of China's largest corporations, notably Alibaba and Tencent, has integrated AI and big data in ways that are changing the geopolitics of the world. The companies, under close coordination with the central government, have strengthened the state's control over its citizens and, in a way, became modern-day "feudal lords" within China.

For instance, Tencent's WeChat platform, used by over one billion people in China, basically holds a

monopoly in the market, which makes WeChat the "dictator" of China's digital space. Moreover, Tencent shares its users' data with the central authorities, backed by the government, which has resulted in quite several arrests. In this example, there is an intersection of state surveillance and private data collection. The systems are used to control and monitor individual citizens.

The government achieves this control through technological means such as AI and big data, which are largely fueled by the data collected by private technology firms. The fact that the government can easily get hold of the data it needs from these companies shows how central data collection is to this system and how tech firms have become de facto "feudal lords" of the digital age.

Much of the AI research in the United States is driven by private companies, including OpenAI and Google DeepMind, which have taken the lead in developing autonomous systems that could alter industries across the world. As these technologies become more deeply embedded in national defense, health, and infrastructure sectors, those controlling AI systems will hold an influence without precedent across borders. This has made some commentators speak of a race toward Artificial Intelligence as the new "arms race" of our era.

It is worth noting that different companies employ varying strategies in this AI race. For example, Meta has open-sourced its LLaMA AI, allowing individual developers to "fine-tune" it and push the technology to new levels of sophistication. This open-source strategy is effective, but it is important to emphasize the fundamental difference between AI and AGI (Artificial General Intelligence). The AI developed by companies like Google, OpenAI, and Meta is primarily classified as "Narrow AI (NAI)," which excels in performing specific tasks, such as image recognition, translation, and playing chess. However, NAI is still far more limited compared to AGI.

AGI, or Artificial General Intelligence, is considered the closest form of AI to human intelligence and represents true transformative power. Currently, AGI is still evolving, with its components in various stages of development. Once fully realized, AGI could bring about a radical shift in the global balance of power, fundamentally altering the reality we live in. A key consideration here is that while many individuals and smaller firms can create and use NAI systems, AGI requires vast financial resources, data, energy, and other inputs—resources that are typically only accessible to large corporations. These corporations possess the most valuable asset in the development of AGI: data. The importance of data in this context cannot be overstated, as it only amplifies the power of these companies.There is an increasing tendency for those companies to assume an almost political role. For instance, Meta exercised a political authority that nation states have over their citizens when it applied a ban to political leaders and erased content inconsistent with its policies. In the same vein, the policies which Amazon applies to its supply chains and the labor force changes the economies of countries around the globe. Consequently, the need for new governance systems that can respond to the new challenges posed by these corporations has emerged. Multilateral organizations such as the United Nations and the World Trade Organization are having difficulties adjusting to this new situation, whereby global power is no longer able to be defined purely in terms of state actors but also in terms of corporate entities who control the broadband networks and data systems. A section of the academia believes that new regulatory protocols at the international level will be needed in order to rein in the global influence of certain technology firms.

Echoes of the Digital Cold War

The 20th century witnessed a struggle between the two big winners of World War II, the USA and the USSR. It was, in effect, a struggle to determine the future world order and which of the two ideologies—capitalism or communism—would dominate. While the Cold War spanned from the end of World War II through the late 20th century, in the end, capitalism triumphed after the fall of the Soviet Union. The turn of the 21st century was marked by quite a number of changes in the landscape of politics and international relations, norms, values, foreign policies, and priorities of the states. Today, in international relations, the new term is the "New Cold War," which differs much from the previous one. This time, it is between the U.S. and China. Some even go to the extent of saying that the war is not real but the making of writers, security experts, and think tanks. A more realistic view should say otherwise. It is not a traditional Cold War, but a "Data/Digital/Virtual" Cold War, where the country holding the greatest amount of data and most advanced computational technology will surely be the one leading world power dynamics. During the classic Cold War, nations focused on military

modernization, stockpiling of nuclear weapons, and increasing defense budgets. But since then, the focus has shifted to the rapid advance of artificial intelligence, which is now having profound global consequences (Shoshana, Z., & Guo, D, 2019). Technologies like 2G and 3 G are fast being replaced by 5G and even 6G, heralding a new era of digital competition and technological arms races that will have wide-ranging implications for the world's power structures and security.

As we go deeper into this epoch of the digital Cold War, it's not just a matter of the U.S. and China being the major players; we all are part of this real digital political world. Artificial intelligence has advanced far beyond what was once imagined. Social apps like WhatsApp, Facebook, Tinder, Twitter, and communication devices like mobile phones and SIM cards have become tools for collecting massive data. We can't ignore the fact, in this digital age, that we are under surveillance, being trapped in this "prison" made by smartphones, social media apps, and the AI system. This is about personal data and sensitive information that are always at risk of exposure or leaking through these platforms. Now, everything is moving toward digitization and deep integration of AI with technologies; it will change global dynamics. Digital governance, digital warfare, digital space conflicts, digital terrorism, and even digital globalization are now rewriting international relations. This digital transformation is rapidly remaking the world, where data and technology are divining power. China has been moving strategically in computational technologies, not repeating errors that the USSR did during the Cold War. The nation is not looking for conflict with its neighbors or the USA, as it follows its vision of a harmonious and peaceful world. China has recently successfully tested its artificial sun, which is going to be a massive innovation and could prove transformational in the 21st Century. At the same time, the USA is also advancing its technology on all fronts. Given the complexity of this digital cold war, it is unbelievable but for the fact that the race between the US and China is not a traditional military and ideological conflict but rather one where control over data and technological prowess is shaping the future of global power. Spillovers abound in the different facets of international relations, from governance and security to societal norms. It is in this potential that open and surreptitious conflict may happen as nations from all over the world strive for technological supremacy. The digital landscape is more than just a backdrop to contemporary geopolitics—it is one of the arenas where the future of global order will be contested. Therefore, it is of the utmost importance that the shades of this new cold war be understood by policymakers, scholars, and citizens alike, as all of us together address this challenge and opportunity brought about by an increasingly interconnected and digitized world(Mueller, M. 2013).

Examples of New Tech Cold War Between U.S.A. and China

With escalating "Tech Cold War" between the United States and China in recent times, restrictions have been imposed on Chinese tech companies including Huawei, as well as pressuring European nations to shun plans involving Huawei for 5G network deployment. As another example in this direction, Huawei was banned from using the Android operating system on the grounds that Google, under the influence of both Google and the Trump administration, was engaged in espionage activities through programs added to the Android system in the technological devices it produces. By the company Huawei. There are also accusations that Huawei has added “backdoors” (Nixon, M, 2022). In addition to espionage, information warfare and technological warfare should also be emphasized here.

However, this dispute is not only from national security concerns or Trump’s aggressive actions; it is more about the difficulty faced by the U.S in maintaining its technological leadership when the cloud capital has already surpassed traditional physical capital. When Joe Biden assumed office, the New Cold War with China intensified, especially in October 2022. As reported by The New York Times, the Biden administration imposed sweeping restrictions on the sale of semiconductors and chip-making equipment to China, aiming to block the nation’s access to key technologies. In essence, Biden's message to Beijing was clear: the United States would thwart China’s ambitions of developing a technologically advanced economy (Swanson, A, 2022).

In order to comprehend the origins of this conflict, it is necessary to return to the tale of the Minotaur. After the Nixon Shock in 1971, the United States left the gold standard so that the dollar could float freely in the international financial arena. This had resounding effects on the international monetary system because other countries" central banks had to hold US dollars instead of gold against which their own currencies could be

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

pegged. The dollar was turned into an IOU and therefore through one hegemonic power, which was realized as America, the global system of finance seemed to be nothing more than a series of promises. A "magic formula" had been found by the U.S, which enabled convincing rich foreigners along with central banks of foreign countries to sponsor its government and imports simultaneously, voluntarily. This way, trade surpluses from countries such as China and Germany were channeled into the U.S productive investments and the system was denoted Minotaur. These monetary inflows or rather tributes to the Minotaur were essential in keeping peace and ensuring global prosperity up to the time when, because of the financial crisis in 2008, they made the system fall apart. The United States does not just attempt to dominate because they fear losing control over their territory; instead, it is part of their old policy of dominating foreign capitalists. The country has always spelled out its restrictions for outsiders, including disallowing them from obtaining important American enterprises like Boeing, General Electric, Big Techs, Big Pharmas or major banks. This crackdown on Chinese tech companies today is a modification of this old scheme after the 2007-2008 crisis, where cloud capital became global and could realize value from all corners.

On May 10, 2019, the United States raised the tariff on Chinese goods from 10% to 25%, most significantly affecting technology products, particularly smartphones and computers. According to data from 2018, the U.S. imported $539 billion worth of goods from China. Topping the list were mobile phones and similar devices. In second place were computers followed by telecommunications equipment, computer accessories, and toys and games. Notably, 40% of the total value of the 140 Chinese imports comprises only five product categories from the tech sector. The mention of the words 'United States', 'China', and 'Phone' immediately evokes the notion of 'Apple's iPhone'. iPhones are manufactured in China and then shipped worldwide. The 25% tariff rise was meant to pressure Apple into moving iPhone production out of China (Haberturk, 2019). Whereas China has the advantage of lower production costs, Apple has been toying with the idea of restricting China to just assembly and making components of the iPhone in countries other than China. From the view of China, the oft-repeated legend "Designed by Apple in California. Assembled in China" has turned into a product "Designed and Assembled in China" due to tremendous strides in technology. From manufacturing fake products, Chinese brands have emphasized selling their original innovative products. In fact, according to October 2024 data, Chinese companies that previously struggled to make the list of the world's 20 largest technology companies are now relatively well represented. However, in the list of the 20 largest companies by market capitalization (Tencent and Alibaba), there are only 2 Chinese companies. The US has absolute hegemony here, but 20 years ago it was very difficult to see a Chinese company even in the top 100 (Du, T, 2022).

Table 1 : Largest tech companies

1	Apple	$3.556 T	USA
2	NVIDIA	$3.469 T	USA
3	Microsoft	$3.206 T	USA
4	Alphabet (Google)	$2.097 T	USA
5	Amazon	$2.000 T	USA
6	Meta Platforms (Facebook)	$1.490 T	USA
7	TSMC	$1.023 B	Taiwan
8	Broadcom	$832.01 B	USA
9	Tesla	$830.37 B	USA
10	Tencent	$494.67 B	China

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

11	Oracle	$480.30 B	USA
12	Netflix	$325.88 B	USA
13	Samsung	$286.50 B	S. Korea
14	Salesforce	$285.90 B	USA
15	ASML	$284.67 B	Netherlands
16	SAP	$282.43 B	Germany
17	AMD	$265.77 B	USA
18	Alibaba	$239.22 B	China
19	Cisco	$222.43 B	USA
20	Adobe	$213.43 B	USA

It is also worth noting that the US ranks first in the market capitalization comparison of technology companies. In other words, only 40 of the top 100 companies are not US companies. In other words, about 60 percent of the global technology market is controlled by US companies. This version is a more succinct and emphasized expression of US technological superiority.

As we mentioned, although Chinese companies did not appear on the global stage in the 2000s, they are very prominent today. Thus, in the list of the 100 largest companies by market capitalization in October 2024, China is represented by 9 companies and is the closest competitor of the US. The market capitalization and ranking of Chinese companies are as follows:

Table 2 : Largest Chinese tech companies

10	Tencent	$494.67 T	China
18	Alibaba	$239.22 T	China
26	Pinduoduo	$173.84 T	China
31	Meituan	$147.27 T	China
53	Xiaomi	$82.63 T	China
67	Jingdong Mall	$61.83 T	China
74	MicroStrategy	$51.97 B	China
80	SMIC	$48.01 B	China
89	Trip.com	$42.45 B	China

Although U.S. companies still dominate the top of the global tech list, the rapid progress of Chinese companies is remarkable (Companies Market Cap, 2023). In 2023, China's digital economy will grow at a growth rate of 10.3% to $7.5 trillion, accounting for 42% of total GDP, and interestingly, China's digital economy showed a higher result, accounting for 7.4% of the country's nominal GDP. Here we see China hegemonizing the US over the digital economy(Statista,2023). In other words, the US digital economy will be 2.57 trillion dollars in

2022, which is about 3 times less than China's digital economy. When we look at the share of the digital economy in GDP, it is 42 percent in China and 10 percent in the US (Sherrill, M, 2024).

As can be seen here, China's digital economy differs significantly from the US. China's investments in the digital economy mean that in the future, China will take China further ahead, while leaving the US further behind. As an example of this difference, China's massive investments in 5G infrastructure are also supporting the rapid development of artificial intelligence, IoT and other technologies. At the same time, it should be emphasized that the Chinese government's incentives in this area are also very important. It is important to note here that China's data-centric and data-driven approach will not only carry China into the future technologically, but also that investments in big data analytics and artificial intelligence applications will increase business efficiency and create new business models. . Overall, these powerful and comprehensive strategies suggest that China will not only close the gap with the US in the future, but will also lead the way in this area. Deep learning and data-driven approaches to AI development are further strengthening China's digital economy hegemony.

In fact, Alibaba, a Chinese company, owns the world's most valuable AI startup. Nowhere is this commitment to AI development more reflective than in the fact that the Chinese government has even introduced AI textbooks into the curriculum of high schools. China, which has filed five times more patent applications in artificial intelligence than the United States, now leads the world in the production of academic articles on AI. With strengths in "deep learning" and "data" under the AI umbrella, China has entered a new phase of "technology wars" with the U.S. The increasingly fierce competition in technology and internet between the two countries is put into focus in Table 3, which looks at how both have progressed and who has more influence in these fields.

Table 3 : Comparison of United States and Chinese-based companies

Search Engine	Google	Baidu
E-Commerce	Amazon, eBay	Taobao, JD.com, Tmall, Temu
Video	Netflix, Hulu, YouTube	Tencent Video, iQiyi, Youku
Music	Apple Music	KuWo Music, KuGou Music
Social Media & Messaging	WhatsApp, Facebook, Twitter, Instagram, Snap	WeChat, QQ, Weibo, Tiktok
Ride-Sharing	Uber, Lyft	Didi
Home-Sharing	Airbnb	Xiaozhu
Dating	Tinder	Momo

China has developed several key systems for collecting the vast amounts of data necessary to advance its artificial intelligence capabilities, with the Social Credit System standing out as perhaps the most significant (H.Kerem Fındık, 2018). This system, mandatory for all citizens, continuously monitors daily activities, evaluating and categorizing individual behaviors as either positive or negative. Through its integration with platforms such as Alibaba, Temu, and WeChat, the system enables China to track global market trends and gather detailed information about citizens' dietary habits, hobbies, daily routines, and even urban planning. The Social Credit System can be aptly characterized as a form of "digital dictatorship," as it centralizes control over citizens' behaviors and societal participation. Intriguingly, it parallels the dystopian scenario depicted in the "Nosedive" episode of the 2016 series Black Mirror, in which individuals rate each other via smartphones, and these ratings dictate social standing and access to opportunities. In China, however, the process is far more institutionalized, with the government assigning and managing these ratings, thereby determining the level of social and economic access each individual can enjoy. This combination of extensive data collection and

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

centralized control positions the Social Credit System as a critical tool in China's broader AI strategy, reflecting both its domestic governance model and its aspirations to lead in the global AI race.

The root of the competition between the U.S. and China in AI and technology is their different approach to innovation, governance, and the use of data. Giants like Google, Amazon, and Facebook lead in the development of AI with a market-driven, innovation-oriented model in the United States. These large private companies operate relatively free from government regulation, using consumer data to promote services that are tailored to the individual, machine learning, and autonomous systems. It is led by the private sector, orienting consumer satisfaction and cutting-edge technology to keep pace with global competitiveness. In comparison, China took the state-driven and centralized model with major companies like Baidu, Alibaba, and Tencent working close to the government's side. Not only are platforms like WeChat or Temu huge economic powerhouses, but they also become tools for data collection and analysis in serving the state for broader purposes. The Social Credit System is the crown jewel of China's integration of AI into governance, based on data collected from these platforms to regulate social behavior and economic activity. This system, embedded in China's "New Generation AI Development Plan," is shorthand for the government's ambition to use AI for national interests, including economic growth, security, and global influence (Redirect Notice, 2024). The competition between the U.S. and China, therefore, goes far beyond a simple competition for technological supremacy. The U.S. focuses on a decentralized, private-sector-led approach that emphasizes individual innovation, while China prioritizes data sovereignty and government-aligned AI applications to assert control domestically and globally. This divergence not only shapes the development of AI but also intensifies geopolitical competition, as both nations vie to set the standards and norms for AI governance and technology deployment in the 21st century.

Huawei sold around 240 million smartphones in 2019 compared to Apple's 197 million. It also means that Huawei took Apple over as the second-largest smartphone maker in the world. A year later, Huawei even managed to capture 10% of the smartphone market in 2020. Thus, its market share, which was 2.52% in 2015, quadrupled in the next 5 years (Villas-Boas, A, n.d). However, many bans, such as Google's ban, caused Huawei's decline, and its market share, which started to decline from 2020, reached the same level in 2024 as in 2017, hovering around 3.71%. It should be emphasized here that in the “Mobile Vendor Market Share” list for 2024, although Apple (28.33%) and Samsung (22.8%) have 51% of the market, China-based Xiaomi (10.64%), Vivo (5.68% of the market) and Oppo (5.4%) control 21.72% of the marke t(StatCounter Global Stats, 2024).

As for the reasons for these bans on Huawei, there are many. Firstly, a key concern for the Western world and the United States is Huawei’s ties to the Chinese military. Its founder, Ren Zhengfei, is not only a member of the Chinese Communist Party but also an engineer with military service. This relationship has led to worries about privacy, as the West believes that if Huawei were requested to share information collected from other countries, the company would not be able to ignore such demands. Another concern in the Western world is that Chinese companies Huawei and ZTE's operations in the United States could allow communications to be monitored, exposing the risk of cyberattacks on critical infrastructure and facilities such as the power grid. The international organization comprising the intelligence agencies of the United States, the United Kingdom, Australia, Canada, and New Zealand is known as the "Five Eyes Alliance." (The National Counterintelligence and Security Center, 2024) Initially established during the Cold War to monitor the Soviet Union and the Eastern Bloc, the alliance shifted its focus to counterterrorism following the Cold War's conclusion and has recently directed its attention toward China and its overseas activities. As the United States works to enhance the security of its 5G supply chain, its pressure on Germany and the UK explicitly conveys the message to "stay away from Huawei." In the Donald Trump administration’s time, their sanctions on Huawei and the support of major American technology companies in this decision are aimed at seriously harming Huawei as a player in the global smartphone market. With this move, Huawei was forced to limit its sales to the Chinese market, even if it can produce phones independently of the parts it sells to American companies (Koshar.A,2019). However, US sanctions didn't kill Huawei—instead it made it stronger. Huawei replaced some 13,000 foreign-produced components that exist in its devices with others made in China, in some cases it had to step up and develop them itself as alternatives didn’t exist. It developed new operating systems for its smartphones and laptops—that’s HarmonyOS—and even more obscure tech such as its own ERP software as Oracle was prohibited from working with the firm (The Economist,2024). Huawei owns a strong position in

the Q2 2024 global foldable market. Among various regions, Asia-Pacific appeared as the fastest-growing market for foldable. Huawei folding phones are performing great in these global regions for Q2 2024. The company appeared in the top three rankers for the Asian markets (IamZen,2024).

Thus, in this new world, there are the cloud capitalists of China stalking the U.S. The latter country, being the leader in terms of technology, is facing a huge challenge from China. The U.S. has started to curtail Chinese tech companies like Huawei, which pressurizes European nations not to involve Huawei in their 5G network project. These measures are not only meant to address security issues but also as a desperate bid to keep American technological superiority in an age where things are different. The prize for which the U.S. and China are fighting in what experts describe as the "Tech Cold War" is controlling the future of cloud capital, and the U.S. will do its best to win at all costs. This is a game of dominance, where the US is trying to keep its lead when the established rules have lost their relevance—its consequences will be felt in every economy and international relations. Finally, the "Tech Cold War" is really a symptom of a much deeper problem the US has had to grapple with: its inability to come to terms with a world in which cloud capital has replaced traditional physical capital. It is very important that America understand its supremacy can no longer be taken for granted, and it must fight against other rising powers like China if it wants to remain ahead in the race of technology development.

A Survey Approach

Data and Methods: This study employs both quantitative and qualitative approaches to explore contemporary perceptions of techno-feudalism and the Digital Cold War. The combination of these approaches ensures a comprehensive analysis: the quantitative aspect allows for statistical evaluation of trends and correlations, while the qualitative approach provides deeper insights into respondents' perspectives. The justification for this mixed-method approach lies in the nature of the research questions, which require both numerical data and interpretative analysis to assess evolving global power structures.

Research Methods: The quantitative component of this study is based on a structured survey administered to a targeted sample. The survey includes Likert-scale questions measuring perceptions of techno-feudalism, the role of technology companies, and state influence in the digital economy. These numerical responses enable statistical evaluation of dominant trends.

The qualitative aspect is integrated through open-ended responses, allowing participants to elaborate on their views. This method enables a nuanced understanding of the socio-political implications of digital power shifts.

Data Collection and Participants: The survey collected 64 responses from individuals across various educational backgrounds, including bachelor's, master's, and PhD students, as well as associate professors. This diverse sample enhances the validity of the findings, as respondents with advanced academic expertise can critically assess and interpret the research themes.

Participants were recruited through Google Forms, using academic networks and professional connections to ensure a high level of engagement. The data is primary, collected specifically for this study, making it directly relevant to the research objectives.

Data Analysis Strategy: The quantitative data was analyzed using descriptive statistics, including frequency distributions and percentage breakdowns of responses. Key survey questions were examined to determine the extent of agreement with the techno-feudalism hypothesis, the balance of power between technology corporations and states, and the perceived influence of AI in the Digital Cold War.

For qualitative analysis, thematic coding was applied to open-ended responses, identifying recurring patterns and divergent viewpoints regarding the evolving role of technology companies.

Results: Key findings include:

- 73.44% of respondents strongly believe that a Digital Cold War is occurring.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

- 81.7% affirm the concept of techno-feudalism, supporting the idea that technology corporations function as new “feudal lords.”
- 74.3% fully agree that the global economy is controlled by a few dominant technology and financial companies.
- Regarding state versus tech company power, 50.8% perceive states as more powerful, while 28.9% see technology firms as dominant.
- 60% of respondents believe that the Digital Cold War negatively affects global stability but remains manageable.

Discussion: These results align with existing literature on digital monopolies, economic restructuring, and power shifts in the international system. The findings provide empirical support for the argument that technology companies are emerging as dominant geopolitical actors, challenging the traditional supremacy of nation-states. Furthermore, the analyses confirm the research hypotheses regarding the increasing role of techno-feudalism in global capitalism. The survey findings substantiate prior theoretical work by demonstrating widespread recognition of technology corporations' economic and political dominance. This study contributes to the growing discourse on AI, digital sovereignty, and techno-feudalism, offering empirical insights that reinforce the urgency of addressing corporate power in global governance.

For our scientific research, a questionnaire was carried out, aiming at the key elements highlighted during the study, and the questions were formulated according to the research goals. The responses to these questions revealed some critical aspects. First, the questionnaire obtained 64 responses, ranging from bachelor's to master's and PhD levels, besides associate professors. This number demonstrates that the scientific value of the questionnaire is satisfactorily substantial. Furthermore, the high level of educational background of most respondents gives more validity and credibility to the results and scientific evaluation of the survey. Hence, the data of this research might be able to successfully present contemporary trends and prospects in the evolution of the discipline. This added to the higher educational level of the participants, making them even more capable of analyzing the subjects more deeply and relating them to already known scientific knowledge. In one of our questions, we asked if a Digital Cold War is currently taking place, and the results showed that 73.44% of the respondents answered between 7 and 10, indicating belief in the presence of a Digital Cold War in today's world. In contrast, only 9.38% of the respondents, whose responses were between 0 and 4, did not support this view. Moreover, an examination of the overall responses lets us conclude that our study is highly relevant and timely.

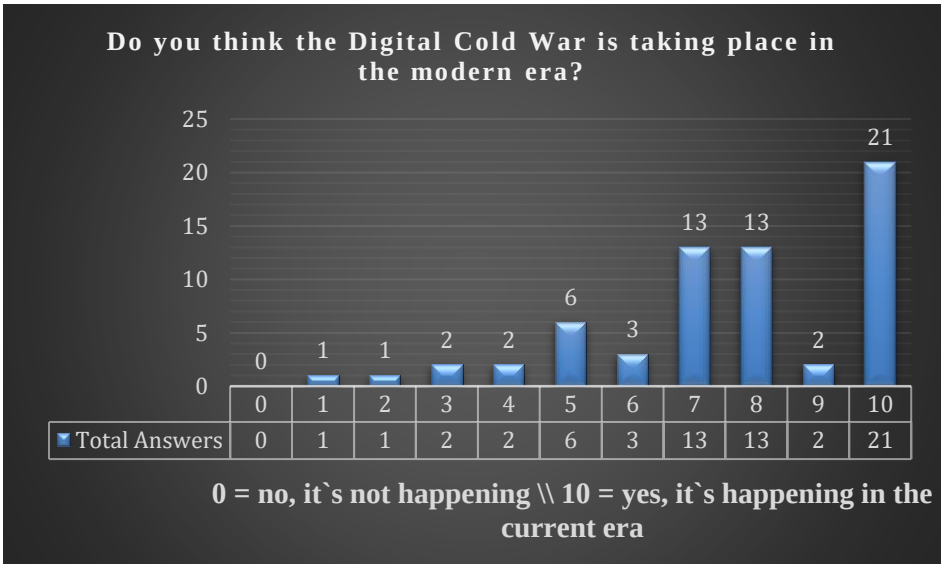

Table 4

To this survey, we added a question regarding the techno-feudalism assertion that is said to be arising in

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

contemporary capitalism where technology companies are the "feudal lords "and people using their services are the "vassals." (Table 4) Generally, 81.7% of the respondents answered (by saying strongly or somewhat yes) affirming the assertion of techno-feudalism stating that contemporary capitalism is helping to bring forth a new socio-political order. A tiny 3.3% rejected the theory, whereas 15% said they were unsure of the concept. These results agree with the massive rise in the power and influence of technology companies in the contemporary economic structure which validates the crucial need to undertake further research work on this particular topic. The findings also highlight the important role played by techno-feudalism theory in modern capitalism analysis and in exploring its mechanisms of structures. In the text of the article, these data come in handy with our views regarding the idea of the economic and social power of technology corporations and how this power is taking form in a very unique way compared to traditional economic systems. This article argues that society is currently undergoing a transitional process toward techno-feudalism, which represents a profound systemic transformation and suggests an overall decline in the role of states as the leading actors(Google Form, Taghizade , E., & Ahmadov, E. 2024).

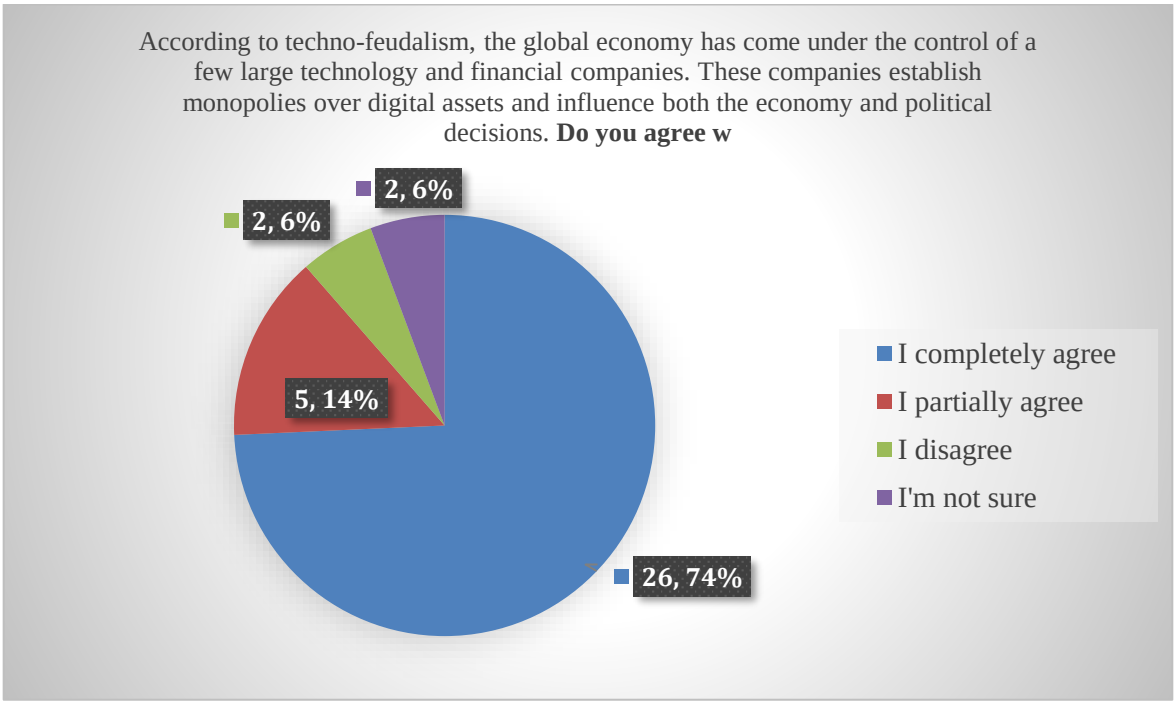

Table 5

Our survey also found strong support for the idea that the modern global economic system has come under the control of a few large technology and financial companies (Table 5). According to the theory of techno-feudalism, the global economy is either transitioning to or has already been dominated by a limited number of major technology and financial corporations. These companies create monopolies over digital assets and influence both economic and political decisions. We further argue that we are in a transitional period toward this process, where large companies may not yet dominate all sectors but hold supremacy in most of them. In this context, the survey responses largely converged on a unified conclusion. Specifically, 74.3% of respondents fully agreed, and 14.3% partially agreed that the global economy is controlled by a few large technology and financial companies, which establish monopolies over digital assets and influence economic and political decisions. Only 11.4% either disagreed or expressed uncertainty on the subject. This indicates widespread recognition of the growing global influence of technology companies. Overall, the survey results reveal that the majority of participants believe the theory of techno-feudalism accurately explains the changes occurring in the modern global economy. A high level of support, at 88.6%, confirms the idea that major technology and financial companies have become dominant forces in the global economic system. This underscores the growing impact of technological platforms, the monopolies they create over digital assets, and their interventions in economic and political decisions. In conclusion, the findings support the view that technology companies act as "new feudal lords" in the modern economy, relegating users to the role of "digital vassals." This trend suggests that as the modern economy becomes increasingly digitized, the power and influence of technology companies will continue to expand in the future.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

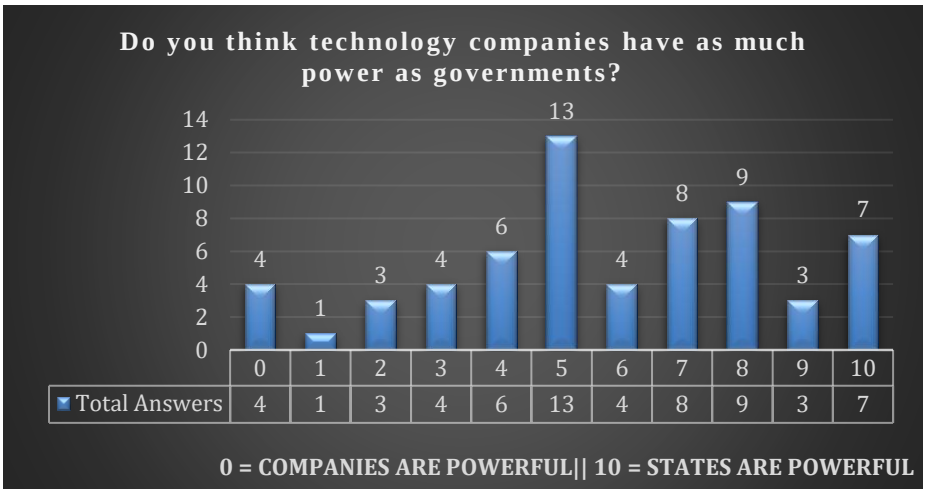

Table 6

In one of the other questions (Table 6) in our survey, we asked whether technology companies or governments have more power in today's world and received some very thoughtful answers. The results indicate that a fair share of respondents believe the balance of power between tech companies and states is more or less equal (21%). In addition to that, 50.8% claim that states are more powerful than tech companies, while 28.9% believe in the superiority of technology companies. These findings support the fact that the global influence of technological companies is constantly increasing and moving closer to the traditional power structures of states. The results of the survey support our proposition that tech companies have turned into powerful influencers, shaping not only the economic environment but also the social and political worlds. Most respondents acknowledge the rising role of technological power in modern society and expect it to continue expanding in the future. At the same time, the analysis shows that while the power of technology companies in global economic and political systems is increasing, they have not replaced state power completely. However, some of the respondents see that in the upcoming years, the growing prominence of technology firms can allow them to become competitors against nation-states. In addition, it is vital to establish that factors like the inadequacies of existing legal systems in the world, their slow operation processes as well as poor regulatory mechanisms contribute vastly to increasing the powers of corporations. These systemic inefficiencies make it possible for tech companies to improve their influence both in global economic and political systems.

We also discussed the issue of the "Digital Cold War" in one of the questions (Table 7), referring to the rivalry between the United States and China in the domains of artificial intelligence and cybersecurity, among others. The question put to the respondents was whether this digital rivalry had a positive or negative effect on global stability. Answers show a differentiated perspective. Roughly 32% of the respondents believe that digital competition severely undermines global stability. Meanwhile, 60% say that even though it has some adverse effects, it can be controlled. Then again, 25% viewed this competition on the positive side in terms of pushing digital and technological developments.

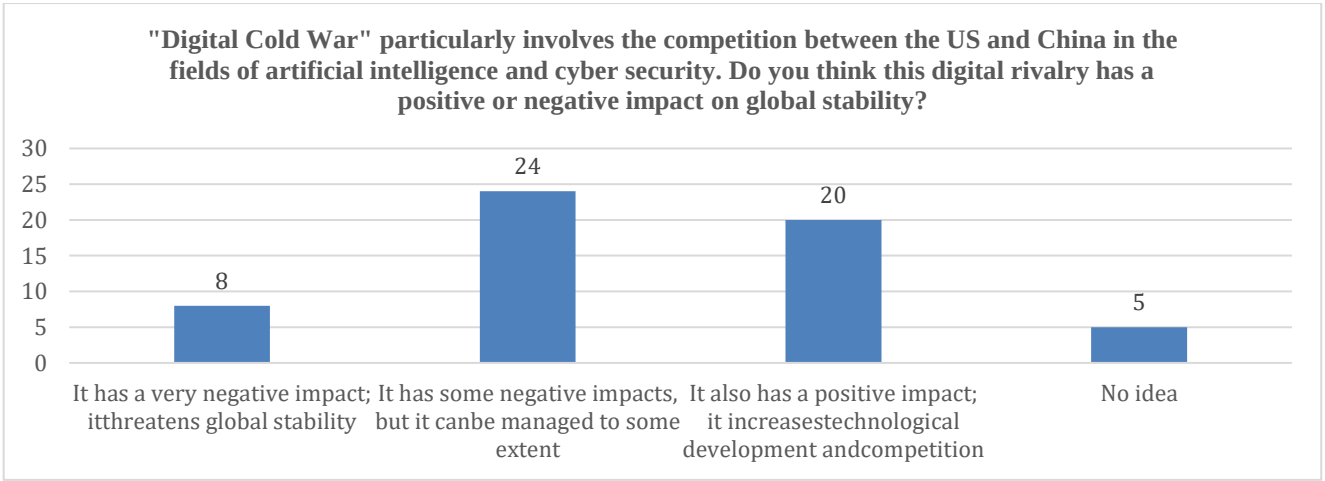

Table 7

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

Finally, approximately 13% felt that it was rather tough to make a judgmental decision. These findings suggest that while many participants do recognize the destabilizing potential of the Digital Cold War, a majority believe that such challenges can be mitigated. Others view the competition in this area as one that could drive technological progress and innovation. This shows that modern global digital conflicts bring about both challenges and opportunities. While respondents generally view the development of digital technologies positively, they stress the need to closely monitor the implications of this rivalry for global peace and stability(Google Form, Taghizade , E., & Ahmadov, E. 2024).

Another question in the survey asked, "How much do you think technology companies influence the decisions taken by governments? " The responses reflect the influence of techno-feudalism in this modern era on the huge power wielded by large tech companies over states and societies. Most of the respondents confirmed that the tech companies have really emerged as global power players, though they emphasized that states are the biggest authority. Indeed, 70% of them believe the influence of tech companies is moderate, while states still hold the reins. Within the "Digital Cold War" framework, while many respondents view the U.S.-China rivalry as damaging to global stability, others realize it has driven economic technological progress and innovation. This agrees with techno-feudalism theory, which likens large technology companies to a challenge to economic and political stability.

Interestingly, most respondents find it unlikely that Chinese applications will outcompete U.S. ones in the global market, hence opening the way for future power shifts in the technological power centers. Moreover, 82% of respondents agree with the fact that technology companies are expanding their economic and political influence, corroborating the techno-feudalism theory's premise of corporations playing a dominant role in these spheres. Taken in sum, these results confirm the relevance of techno-feudalism in explaining the rising dominance of technology companies in global markets. While states still retain some capacity to influence and control these corporations, the latter's increasing power speaks to a shifting balance of influence across the world.

Ultimately, the survey - Table 8 results emphasize the monopolistic tendencies of technology companies in the digital and global economic landscape. Considering that 51% of respondents agreed on the fact that such companies have built quasi-monopolistic positions in the digital economy, findings confirm the notion of techno-feudalism where large technology companies act as quasi-feudal lords by means of holding dominant control over digital assets and user dependency. Of course, absolute monopolies are not formed yet since there still exists competition in some aspects, though those companies hold remarkable dominancy. Today, tech companies are creating monopolies of the global economy and digital world. Within this context, the results of the survey illustrate opinions consistent with techno-feudalism theory, which proposes that tech companies are in a position of authority within the global economy and digital world. According to the results, 51% of participants believe that tech companies have been able to create their monopolies within the digital economy and international markets have a huge influence. It says a lot about how big tech companies position themselves as "feudal lords" over digital assets and their attitudes toward making users dependent on them from a techno-feudal standpoint.

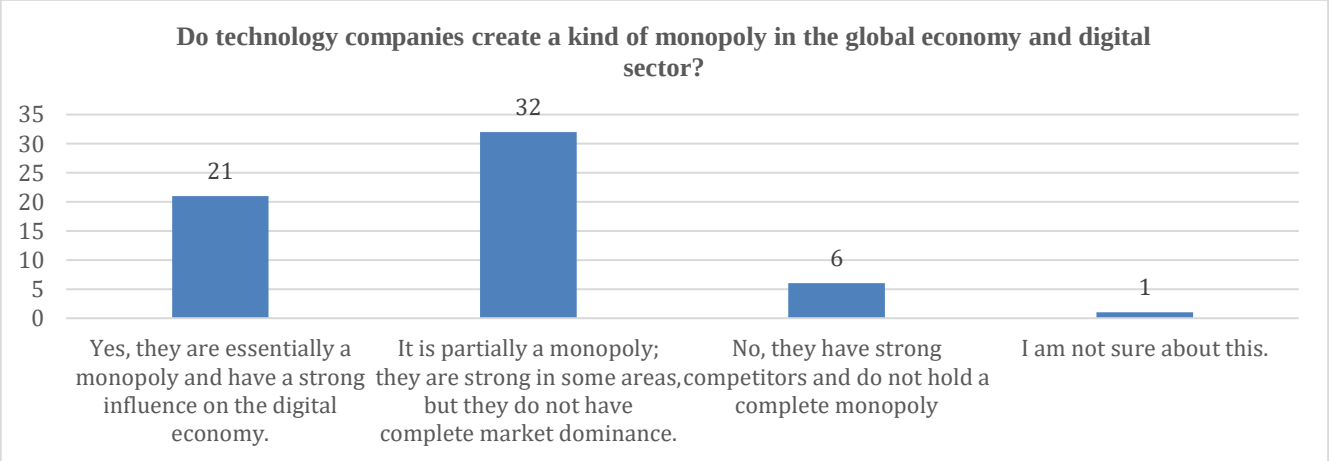

Table 8

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue II February 2025

Also, 46% of respondents insist that tech companies do dominate certain fields but have not gained complete monopolies, and therefore there is still competition. Such an opinion proves that techno-feudalism hypotheses are not widely accepted: some participants feel that competition still exists and did not achieve absolute hegemony. Only 3% of the respondents partaking in this questionnaire were unsure about this issue; hence, techno-feudalism is an argumentative but subtle topic that has to be discussed further.

In a nutshell, this data confirms the main ideas of the techno-feudalism theory with regard to the monopolistic role of tech companies in the world economy and the digital sector. The aforementioned companies still do not stand at the full monopoly level but rather gain great hegemonic control by dominating a great share of the market while keeping influence over users and other actors of the economy(Google Form, Taghizade , E., & Ahmadov, E. 2024)..

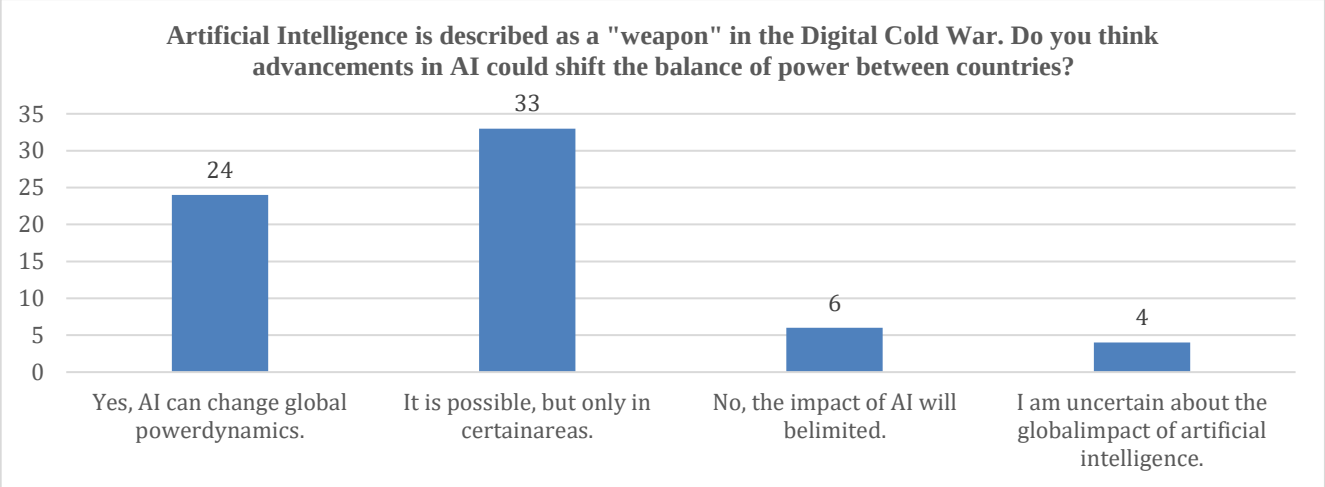

Table 9

We also had a question in our survey related to the use of Artificial Intelligence as a "weapon" in the Digital Cold War (Table 9). We asked how this process might affect the balance of power among nations. Looking through the lens of techno-feudalism at the results of our survey, it's obvious that the huge tech companies are the main actors in the creation of emerging technologies, specifically AI. Any development in AI only increases the digital power of these companies and could have an impact on state sovereignty. The results of the survey bring out the fact that further technological advancement in AI by tech firms can change the global balance of power to turn them into much stronger contenders concerning international relations. If AI is used, for example, in military technologies and cybersecurity, then that would really be an augmentation of the power of the technology companies over states, bringing closer to reality the possibility of a scenario within the techno-feudalism framework where modern societies' structures are more threatened(Google Form, Taghizade , E., & Ahmadov, E. 2024).

In this regard, AI is seen as a very powerful "weapon" in the context of the Digital Cold War because its use can change the military and economic capabilities of nations. Such changes in the global balance of power are likely to create new and distinct forms of competition among states. Many respondents, according to the survey results, pointed to how AI might change the balance of power in some domains—for instance, military operations or information warfare—in ways that would make the technology relevant within the Digital Cold War context. Another view, probably more common, is that the AI effect may be experienced only in certain sectors or under specific conditions. It reflects current uncertainties and risks associated with the global use and impact of AI.

These respondents to the poll hold the view, by and large, that such AI development could change the global balance of power. However, some of the respondents commented that this probably would be less profound and felt only in selected domains. From the perspective of techno-feudalism and the Digital Cold War, the way power dynamics are likely to change—with AI technology growth not only for tech firms but also for states—could spur new strategic competitions where those with greater technological power would have a more significant say in the global politics of tomorrow.

In the conclusion of the survey: The analysis of the survey shows evidence of growing awareness of the serious impacts that technological advancement is imposing on the global socio-economic and political structures. A large portion of the respondents agreed with the statement on techno-feudalism, where technology companies play the role of "digital feudal lords." It also shows from the responses the perceived dominance of technology companies in driving economic systems, with a considerable number of people supporting the assertion of their growing power over traditional state authorities. Notably, the idea of a "Digital Cold War," marked by competition in areas of artificial intelligence and cybersecurity among the world's top powers like the United States and China, found significant support.

Those results, given the high qualification of the participants in education, bring credible views on the detected emerging trends, hence confirming the relevance and scope of the study. These results confirm the growing interconnectedness of technological monopolies, governmental power, and global security, proving the urgent need for interdisciplinary approaches to these problems. This paper contributes to the broader discussion on techno-feudalism and digital globalization and creates a framework for future research in these dynamic fields.

CONCLUSION

In conclusion, the changes brought about by technological developments in the modern world are fundamentally altering socio-economic structures and reshaping international power relations. The concept of techno-feudalism suggests the possibility of the end of the capitalist system and its replacement by a new model of digital governance. In techno-feudalism, traditional economic relations are based on digital platforms controlled by large technology companies. In addition to extracting value from consumers and producers, these power platforms create economic value and play an important role in knowledge management. The emergence of such an economic system raises the question of whether traditional capitalist models and the free market are fit for the future. Here, the control of companies like Amazon, Google and Facebook over vast digital “countries” makes them look like modern feudal lords. These “digital lords” wield unprecedented economic power, often exceeding the GDP of many countries, thus challenging traditional notions of state sovereignty and changing the structures of international relations.

With these developments, the digital cold war between the US and China shows that a new type of competition is emerging as the balance of power shifts. Unlike the political and ideological characteristics of the traditional cold war, the digital cold war focuses more on areas such as cyber security, artificial intelligence and information control. The use of cyber warfare as a new battlefield by state and non-state actors poses great risks to global security and requires states to rethink their national defense strategies. The spread of the digital economy and the growth of global digital connectivity further complicate this conflict and make states more interdependent.

At the same time, we see the sovereignty of states being seriously threatened by or through technological forces. In particular, state and non-state actors are carrying out large-scale attacks against each other through illegal use of data, cyber espionage and information warfare. In modern times, classical wars are on the decline and are being replaced by “cyber wars” that open up new possibilities by requiring the main actors to prepare for the new world. This poses a new threat to national security as countries become more open to external influence in their internal affairs. At the same time, as technology companies gain social and political power, their influence over states is growing. This means that states need to protect their sovereignty not only through traditional military power but also through control of information and digital infrastructure.

This dependence on digital infrastructure and cybersecurity has a profound impact on economic systems. In the era of digital cold war, financial attacks, data leaks and economic breaches have become major threats to global economic stability. In addition to creating an economic crisis, this new situation can lead to rising unemployment, corporate bankruptcies and deepening social problems. Such attacks show that cyber warfare has serious consequences not only in security issues but also in the economic sphere.

Under the impact of techno-feudalism and the digital cold war, global political relations and the international security environment require a new order. In such an environment, states and international organizations have to create new rules and norms. Issues of digital security and control over technology companies require the

formulation of new international rules to mitigate the unjust and threatening effects of the digital economy. Institutions such as the UN and the World Trade Organization need to adapt to this new situation because global power today is determined not only by state actors but also by the companies that dominate the digital economy.

The results of the paper show that technology is driving major changes not only in the social and economic spheres, but also in the global political environment. The rise of digital infrastructure and cybersecurity will have serious implications for global stability and security in the future. States need to develop new strategies to protect their digital sovereignty and rethink their cooperation with technology companies. The key analysis of this period is therefore to consider digital technology not only as an economic force, but also as a central element of global power. As the digital economy grows, so does the competitive landscape on a global scale, and nations must work to redefine their position of power in this new technological era.

REFERENCE

1. ANI. (2013, June 7). Chinese hacked Obama, McCain campaigns, say US officials. Business Standard. Retrieved November 14, 2024, from https://www.business-standard.com/article/news-ani/chinese-hacked-obama-mccain-campaigns-say-us-officials-11360700607_1.html
2. Archondakis, A. (n.d.-b). The Top 5 Most Dangerous Cyber Attacks of all Time. Pentest People. Retrieved from https://www.pentestpeople.com/blog-posts/the-top-5-most-dangerous-cyber-attacks-of-all-time
3. Barbora Jedlickova. (2024, September 9). Google is facing another crucial court case in the US – and it could have major consequences for online advertising. The Conversation. Retrieved from https://theconversation.com/google-is-facing-another-crucial-court-case-in-the-us-and-it-could-have-major-consequences-for-online-advertising-238227
4. BBC. (2017, October 3). Yahoo 2013 data breach hit “all accounts.” BBC News. https://www.bbc.com/news/business-41493494
5. Biddle, E. R. (2015). Decoding the Digital Cold War. Americas Quarterly, 9(2), 93.
6. Biddle, E. R. (2015). Decoding the Digital Cold War. Americas Quarterly, 9(2), 93.
7. Biddle, S., Mutrie, N., & Gorely, T. (2015). Psychology of Physical Activity. Routledge. https://doi.org/10.4324/9780203123492
8. Blessing, J., Post-Doctoral, D., & Fellow. (2018). The Global Spread of Cyber. CCDCOE. Retrieved from https://ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf
9. Bremmer, I. (2021, October 19). The Technopolar Moment. Foreign Affairs. https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order
10. Bremmer, I. (2021, October 19). The Technopolar Moment. Foreign Affairs.
11. Bugcrowd. (n.d.). Night Dragon operation. Retrieved from https://www.bugcrowd.com/glossary/night-dragon-operation/
12. Cadwalladr, C., & Harrison, E. G. (2018, March 17). Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. The Guardian. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
13. Clayton, M. (2012, September 14). Stealing US business secrets: Experts ID two huge cyber “gangs” in China. Christian Science Monitor. Retrieved from https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China
14. CompaniesMarketCap. (2023). Largest tech companies by market cap. CompaniesMarketcap.com. Retrieved from https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/
15. CompaniesMarketCap. (2024). Companies Ranked by Market Cap. CompaniesMarketcap.com. Retrieved from https://companiesmarketcap.com/
16. Conversation. (2022, January 26). Yanis Varoufakis on Crypto & the Left, and Techno-Feudalism. The Crypto Syllabus. Retrieved from https://the-crypto-syllabus.com/yanis-varoufakis-on-techno-feudalism/
17. Dobusch, L., & Kreissl, K. (2024). Techno-Feudalism and Its Discontents. Routledge.
18. Dobusch, L., Dobusch, L., & Kreissl, K. (2024). Chapter 15 Searching for Transformative Potential: Comparing Conceptualizations of Open, Inclusive and Alternative Organizations. The Handbook of

19. Organizing Economic, Ecological and Societal Transformation, 295–314. https://doi.org/10.1515/9783110986945-015
20. Du, T. (2022, October 17). Animation: The Largest Public Companies by Market Cap (2000–2022). Visual Capitalist. Retrieved from https://www.visualcapitalist.com/cp/largest-companies-from-2000-to-2022/
21. Durand, C. (2020c). Technoféodalisme - Cédric Durand - Éditions La Découverte. Éditions La Découverte. Retrieved November 15, 2024, from https://www.editionsladecouverte.fr/technofeodalisme-9782355221156
22. ExecutiveGov. (2024, May 8). 10 Government Cybersecurity Company Contractors. Retrieved from https://executivegov.com/articles/10-cybersecurity-company-contractors/
23. Feingold, S., & Wood, J. (2024, May 15). Cyberattacks Threaten Global Financial Stability, IMF Warns. World Economic Forum.
24. Feingold, S., Wood, J., & World Economic Forum. (2024, May 15). Cyberattacks threaten global financial stability, IMF warns. World Economic Forum. Retrieved from https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/
25. Fox, J. (2022, October 7). 8 biggest cyberattacks in history | cobalt. Cobalt.io. Retrieved from https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history
26. Fortinet. (2023). Top 20 Most Common Types Of Cyber Attacks. Fortinet. Retrieved from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks
27. Goodman, A. (2023). The Conceptual "New Cold War": A Comparative Analysis of Great The Conceptual "New Cold War": A Comparative Analysis of Great Power Competition Power Competition. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1571&context=honorstheses
28. Google Form, Taghizade , E., & Ahmadov, E. (2024, November 14). Share your thoughts on Techno-Feudalism and the Digital Cold War with us (Texno-Feodalizm və Rəqəmsal Soyuq Müharibə ilə bağlı fikirlərinizi bizimlə bölüşün) - First Survey. Retrieved November 14, 2024, from Google Form website: https://docs.google.com/spreadsheets/d/13fCvSLxReb7cJtvyfewQV7MhicJlkIYHAMr2l24kDsQ/edit?usp=sharing
29. Google Form, Taghizade, E., & Ahmadov, E. (2024, November 14). Share your thoughts on Techno-Feudalism and the Digital Cold War with us - Second Survey. Retrieved November 14, 2024, from Google Docs website: https://docs.google.com/spreadsheets/d/1W9P0-AoD3Rp7WSAipFd-fzLOk4FdR4Ahjo6yCc86_ag/edit?usp=sharing
30. Gorman, S., Cole, A., & Yochi Dreazen. (2009, April 21). Computer Spies Breach Fighter-Jet Project. WSJ. Retrieved from https://www.wsj.com/articles/SB124027491029837401
31. H.Kerem Fındık.(2018). US-China tech-driven trade war. Digital Age. Retrieved September 29, 2024, from https://digitalage.com.tr/abd-cinin-teknoloji-odakli-ticaret-savasi/
32. Haberturk. (2019, May 10). US-China trade war could hit iPhone! Technology News. Retrieved September 29, 2024, from https://www.haberturk.com/abd-cin-ticaret-savasi-iphone-u-vurabilir-2458672-teknoloji?page=8
33. Hill, M., & Swinhoe, D. (2022, November 8). The 15 biggest data breaches of the 21st century. CSO Online. Retrieved from https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
34. How To Academy. (2024b, August 11). "This is not Capitalism Anymore!" Yanis Varoufakis on Technofeudalism, Big and Big Tech. (Part 1). YouTube. Retrieved from https://www.youtube.com/watch?v=ZD5DLlxuNWk
35. IamZen. (2024, August 29). Huawei has a strong position in Q2 2024 global foldable market: TechInsights. Retrieved November 14, 2024, from Huawei website: https://consumer.huawei.com/za/community/details/Huawei-has-a-strong-position-in-Q2-2024-global-foldable-market-TechInsights/topicId-306178/
36. Identity database "leak" worries Indians. (2018, January 5). BBC News. https://www.bbc.com/news/world-asia-india-42575443
37. Jedlickova, B. (2024, September 9). Google is Facing Another Crucial Court Case in the US. The Conversation.
38. Jensen, B. (2023). How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy. CSIS. Retrieved from https://www.csis.org/analysis/how-chinese-communist-

party-uses-cyber-espionage-undermine-american-economy
39. Khan, W. J. (2024, November 20). Tech Giants as Emerging Diplomatic Players - Centre for Strategic and Contemporary Research. Centre for Strategic and Contemporary Research. https://cscr.pk/explore/publications/articles/tech-giants-as-emerging-diplomatic-players/
40. Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI. Policy & Society (Print). https://doi.org/10.1093/polsoc/puae012
41. Kinsta(2022) Search Engine Market Share: Who's leading the race in 2022. Retrieved from https://kinsta.com/search-engine-market-share/
42. Kost, E. (2022, December 1). The 8 biggest data breaches in financial services (2021 edition). UpGuard. https://www.upguard.com/blog/biggest-data-breaches-financial-services
43. Markoff, J. (2009, March 28). Vast Spy System Loots Computers in 103 Countries. The New York Times. Retrieved from https://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1
44. Meleouni, C. (2023). Artificial intelligence and its impact in international relations. Journal of Politics and Ethics in New Technologies and Ai, 2(1), e35803. https://doi.org/10.12681/jpentai.35803
45. Mokyr, Joel (1990). "The Lever of Riches: Technological Creativity and Economic Progress.
46. Mueller, M. (2013). Are we in a Digital Cold War? at the GigaNet workshop The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and Networks, Graduate Institute (pp. 5–9).
47. Mueller, M. (2013). Are We in a Digital Cold War? GigaNet Workshop, Graduate Institute.
48. Muhleisen, M. (2018, June). The Impact of Digital Technology on Society and Economic Growth - IMF F&D Magazine - June 2018 | Volume 55 | Number 2. IMF. https://www.imf.org/en/Publications/fandd/issues/2018/06/impact-of-digital-technology-on-economic-growth-muhleisen
49. Muhleisen, M. (2018, June). The Impact of Digital Technology on Society and Economic Growth. IMF F&D Magazine.
50. NBC News(n.d.) Chinese hackers hacked Obama, McCain campaigns, took internal documents, officials say. https://www.nbcnews.com/id/wbna52133016
51. Nixon, M. (202). What does Google's decision to ban Huawei from Android mean for the Chinese tech giant? Molzana. Retrieved November 14, 2024, from https://www.molzana.com/blog/what-does-googles-decision-to-ban-huawei-from-android-mean-for-the-chinese-tech-giant/
52. Plummer, R. (2024, July 19). CrowdStrike and Microsoft: What we know about global IT outage. BBC. Retrieved from https://www.bbc.com/news/articles/cp4wnrxqlewo
53. Redirect Notice. (2024). Retrieved November 14, 2024, from Google.com website: https://www.google.com/url?q=https://www.haberturk.com/abd-cin-ticaret-savasi-iphone-u-vurabilir-2458672-teknoloji?page%3D8&sa=D&source=docs&ust=1730893001374266&usg=AOvVaw00RdjuttNaKxopmLe0gIIH
54. Ritchie, H. (2016, December 30). Read all about it: The biggest fake news stories of 2016. CNBC. Retrieved from https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html
55. Robertson, A. (2023, September 12). US v. Google: all the news from the search antitrust showdown. The Verge. Retrieved from https://www.theverge.com/23869483/us-v-google-search-antitrust-case-updates
56. Schwab, K. (2016). The Fourth Industrial Revolution. New York: Crown Business. https://robscholtemuseum.nl/wp-content/uploads/2022/11/Schwab-Klaus-The-Fourth-Industrial-Revolution-2016.pdf
57. SecurityScorecard((2023, September 9).The Top 7 cyberattacks on U.S. government.https://securityscorecard.com/blog/top-cyberattacks-on-us-government
58. Sherrill, M. (2024, June 26). Trade Fact of the Week: The U.S. digital economy, on its own, would be the world's eighth-largest economy. Progressive Policy Institute. Retrieved from https://www.progressivepolicy.org/trade-fact-of-the-week-the-u-s-digital-economy-on-its-own-would-be-the-worlds-eighth-largest-economy/
59. Shi, T. (2010, April 9). Google withdraws from China. Stanford Daily. https://stanforddaily.com/2010/04/09/google-withdraws-from-china/

60. Shoshana, Z., & Guo, D. (2019). A new cold war? Causes and future of the emerging US-China rivalry. Vestnik RUDN. International Relations, 19(1), 9–21. https://journals.rudn.ru/international-relations/article/view/20848/16812
61. Slonopas, A. (2024, April 16). What Is Cyber Warfare? Various Strategies for Preventing It. APU. Retrieved from https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare/
62. StatCounter Global Stats. (2024). Mobile vendor market share worldwide. StatCounter Global Stats. Retrieved from https://gs.statcounter.com/vendor-market-share/mobile
63. Statista(2020)China: Digital economy GDP share 2020.Retrieved from https://www.statista.com/statistics/1250092/china-digital-economy-gdp-share/
64. Statista(2023, December) U.S. targeted political cyberattacks 2023.https://www.statista.com/statistics/1428610/us-targeted-political-cyberattacks-by-characteristic/
65. Swanson, A. (2022, October 7). Biden Administration Clamps Down on China's Access to Chip Technology. The New York Times.
66. Swanson, A. (2022b, October 7). Biden Administration Clamps Down on China's Access to Chip Technology. The New York Times. Retrieved from https://www.nytimes.com/2022/10/07/business/economy/biden-chip-technology.html
67. The Economist. (2024, June 13). America's assassination attempt on Huawei is backfiring. Retrieved from The Economist website: https://www.economist.com/briefing/2024/06/13/americas-assassination-attempt-on-huawei-is-backfiring
68. The National Counterintelligence and Security Center. (2024). Five Eyes Intelligence Oversight and Review Council (FIORC). U.S. Department of National Intelligence. https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc
69. Toffler, A. (2022). The Third Wave (p. 544). Bantam.
70. Valenduc, G. (2018). Technological Revolutions and Societal Transitions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3180000
71. Varoufakis, Y. (2020, August 31). The post-capitalist hit of the summer. Project Syndicate. https://www.project-syndicate.org/commentary/covid19-and-postcapitalist-economy-by-yanis-varoufakis-2020-08
72. Villas-Boas, A. (n.d.). Huawei sold more smartphones than Apple in 2019 despite the fact that its new phones can't run Google apps — but it's not so surprising. Business Insider. Retrieved from https://www.businessinsider.com/huawei-smartphones-2019-more-than-apple-without-google-apps-2019-12
73. Waddell, K. (2016, January 19). Why Google Quit China—and Why It's Heading Back. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/
74. Wineberg, D. (2025, January 18). Neofeudalism summarized and expanded, as capitalism fades under pressure and from old age. Medium; The Straight Dope. https://medium.com/the-straight-dope/neofeudalism-summarized-and-expanded-as-capitalism-fades-under-pressure-and-from-old-age-de80fc6bbdb7
75. Wineberg, D. (2025, January 18). Neofeudalism Summarized and Expanded. Medium.
76. Wolf, A. (2022, August 25). 10 Notable Cyber Attacks on Government Agencies. Retrieved from Arctic Wolf website: https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies/
77. Worldometer. (2023). GDP by country. Retrieved from WorldoMeters website: https://www.worldometers.info/gdp/gdp-by-country/
78. Yahoo Finance(2023, December 6). 16 most advanced countries in quantum computing. Retrieved from https://finance.yahoo.com/news/16-most-advanced-countries-quantum-131132253.html
79. Zhang, Z. (2022, March 29). Study Confirms Influence of Russian Internet "Trolls" on 2016 Election | Columbia SIPA. Retrieved from www.sipa.columbia.edu website: https://www.sipa.columbia.edu/news/study-confirms-influence-russian-internet-trolls-2016-election
80. Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.