Geopolitics Quarterly, Volume: 21, No 2, Summer 2025 Scopus

PP 312-337

Geopolitics of Cybernetics: Visualizing of Emerging New Power

Sohrab Asgari * - Assistant Prof., Geography Department, Faculty of Social sciences, Payam Noor University, Tehran, Iran.

Received: 08/11/2024 Accepted: 10/04/2025

Abstract

One of the most significant breakthroughs in technology is the evolution of computing sciences and cybernetics. This development has had a global impact, with the widespread use of computer sciences leading to worldwide issues. In the third wave, time and place have become intertwined, eliminating the effects of distance and creating a new version of space. These characteristics have transformed the geography of virtual space into the geopolitics of virtual space.

The findings of this analytical article, conducted using a library method and the strategy of cyberspace geography studies, suggest that the geography of virtual space is an emerging academic topic. When the geography of cyberspace addresses inequality in cyberspace security, it becomes a geopolitical issue. The paper explores how cybernetics is changing traditional notions of power, sovereignty, and conflict. The research also considers the implications of emerging technologies on global governance, the balance of power, and the potential for new forms of cyber-hegemony, concluding with recommendations for future policy and strategic considerations in this rapidly evolving field.

Keywords: Cyberspace, Geography of Virtual Space, Geopolitics of Cyberspace.

* E-mail: s.asgari@pnu.ac.ir

1. Introduction

After inventing the counting machine, which was eventually named the computer, the world entered a new era: the era of virtual space and the World Wide Web. It was an undeniable necessity to explore new dimensions of the newly invented hardware. The political landscape, especially the Cold War, motivated scientific researchers to develop the World Wide Web in order to connect the world and create a global village. The Internet began in the 1960s as a way for government researchers to share information. Computers in the '60s were large and immobile, so in order to access information stored on any one computer, one had to either travel to the computer's location or have magnetic computer tapes sent through the traditional postal system.

Nowadays, the internet has caused many evolutionary changes in the world. Virtual space has altered the lifestyles of human beings, impacting health, financial affairs, education, assembly lines, communication, remote sensing, and more. Welfare is the main outcome of this technology, with even wars and conflicts becoming intertwined with the internet and virtual space. Espionage, combat, and defense are now conducted by cybernetic agents. Virtual space, parallel to real space, presents its own unique issues that differ from those faced by societies in the past. However, the groundwork for insecurity has been laid in the world. While all aspects of human life have been affected by the internet and virtual space, the risk of data loss and technical issues remains a significant concern. One of the main characteristics of the modern age is the shift from real space to virtual space, bringing about new challenges with each change.

The terms "cyber" and "cybernetics" have become essential to our understanding of modern technology and its impact on society. Coined by Norbert Wiener in 1948, cybernetics originally referred to the study of control and communication in animals and machines. Wiener's work laid the foundation for understanding feedback loops and self-regulation in biological and artificial systems, with profound implications in fields such as engineering, biology, and social sciences. As technology progressed, the prefix "cyber" expanded beyond the realm of cybernetics to encompass a wide range of concepts related to digital technology and the internet. For example, the term "cyberspace" was introduced by the science-fiction novelist William Gibson in his book "Neuromancer" (Gibson,1984) and

subsequent novels. Cyberspace was depicted as an artificial environment created and maintained by computers (Ralston and Others,2003:474).

This condition lays the foundation for the transformation of the concept and approach of geopolitics. A new version of geopolitics is emerging: Geopolitics of cybernetics. This type of geopolitics is completely different from the old version. In the old version of geopolitics, all challenges occurred in physical space, but in geopolitics of cybernetics, virtual space is the primary element and battleground. The emergence of new types of battles, for example, has led to the development of new methods of confrontation.

2. Methodology and Related Literature

This research was conducted using an inductive approach and the strategy of documentary studies. It is of an analytical nature and was carried out using a library method. To conduct this library research, the general framework of the research was first determined. Following this, reliable sources were reviewed, and relevant sources were selected and studied from among them. The sources used included internal and external sources, as well as related documents and reports.

The information related to the geopolitics of Cybernetics was collected according to the nature of the research topic, and necessary analyses were conducted. Valid indicators were also used to evaluate the state of resources.

The intersection of geopolitics and cybernetics has gained significant scholarly attention in recent years, reflecting the growing recognition of the digital realm as a vital component of global power dynamics. Castells, in his seminal book The Rise of the Network Society (2009), discusses the emergence of a networked global economy, emphasizing the role of information technology in redefining power structures. Collectively, these literatures underscore the necessity of integrating cybernetic concepts into geopolitical analyses, illustrating how digital technology not only influences power relations but also reconfigures the very nature of state sovereignty, security, and global interactions.

Clarke & Knake in their book: Cyber War: The Next Threat to National Security and What to do about it (2010) explores the implications of cyberwarfare on national security, particularly focusing on the geopolitics involved in defending against cyberattacks.

In book titled: The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats (2019), Clarke and Knake Focus

on the critical issue of cybersecurity as the "fifth domain" of warfare, discussing its geopolitics and the measures needed to protect against cyberthreats.

the book: Cybersecurity and Cyberwar: What Everyone Needs to Know, written by Singer and Friedman provides an overview of the key issues in cybersecurity and cyberwarfare, including the geopolitical dimensions and the impact on global security.

The geopolitics of cybernetics is a rapidly emerging field of study, given the increasing importance of information technology and artificial intelligence in global power dynamics. Scholars such as Joseph Nye (2010) have pointed out the shift from traditional forms of power to cyber power, where states leverage digital infrastructure for both offensive and defensive purposes. Nye argues that the control of information and technological networks is now just as vital to national security as military capabilities.

In addition to Nye, a more recent examination by Lucas Kello (2017) explores the concept of cyber warfare and its implications for international relations. He states that cyber threats transcend borders and challenge traditional notions of sovereignty, further complicating the geopolitical landscape. Kello's work sheds light on how cyber capabilities are reshaping global alliances and rivalries, particularly in the context of great power competition. These scholars collectively illustrate that the cyber realm is now a contested geopolitical space, where states, corporations, and non-state actors vie for control. The interdependence between digital infrastructure and geopolitical strategy points to a future where cybernetic capabilities will play an ever-increasing role in shaping global power dynamics.

3. Theoretical Framework

3-1.Computer and Internet: Symbol of Modern Technology

The concept of computing can be traced back to the early 19th century with Charles Babbage, often referred to as the father of the computer. Babbage designed the Analytical Engine, a mechanical general-purpose computer, although it was never completed in his lifetime. His work laid the foundation for modern computing concepts, such as the use of a central processing unit (CPU) and memory (Gleick,2011:92). In the mid-20th century, the development of electronic computers began in earnest. By the 1970s, personal computers began to emerge, with companies like Apple and Microsoft leading the way. The introduction of the Apple II in 1977 and the IBM PC in 1981 brought computing into homes and small businesses,

marking the beginning of the personal computing revolution. This period also saw the development of graphical user interfaces (GUIs), which made computers more accessible to non-experts (Isaacson,2014:238). In the following decades, the internet and mobile computing further transformed the landscape. The invention of the World Wide Web by Tim Berners-Lee in 1989 and the proliferation of mobile devices in the 2000s have made computers an integral part of daily life, connecting billions of people worldwide (Leiner and Others.2009:39). Like many of the technologies that we take for granted nowadays, it got its start during the Cold War as the U.S. government sought to gain an edge over its bitter rival, the Soviet Union. In 1957 the USSR successfully launched the world's first satellite into orbit, a move that is widely seen as marking the start of an era in which these two global powers battled for technological supremacy. Vinton Cerf and Robert Kahn invented internet in 1970s. The Internet has been widely used since its invention. As of April 2024, there were 5.44 billion internet users worldwide, which amounted to 67.1 percent of the global population. Of this total, 5.07 billion, or 62.6 percent of the world's population, were social media users (www.statista.com).

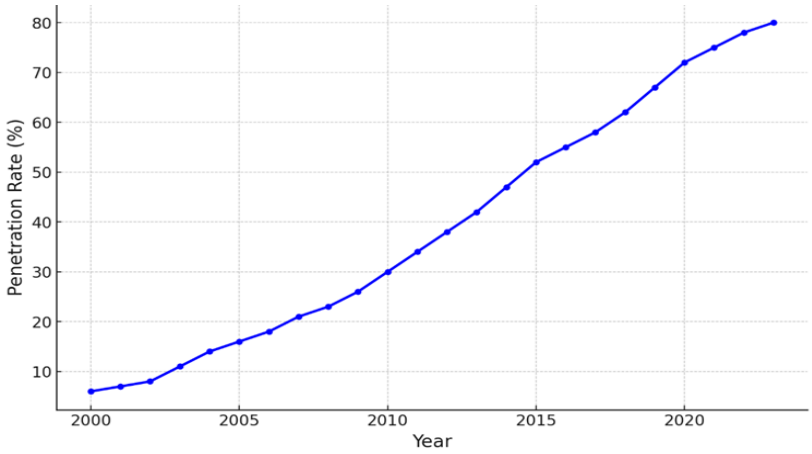

Figure (1): Global Internet Penetration over Time (2000-2023)
(**Source:** Statista.com)

Most of the internet users are Asian residents. Asia comprises more than 40 percent of the world population so its logical to have the most internet users in the world.

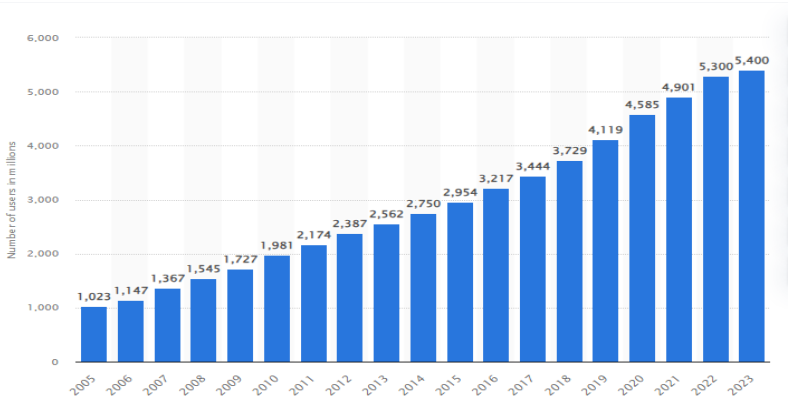

Figure (2): Number of Internet Users
(**Source:** Statista.com)

The world wide web and virtual space are a suitable opportunity that generates power for its controller. The USA, as the founder and primary guardian of the Internet, continues to exert its tangible and intangible control and influence on this network and space and benefits from its economic advantages in its geographical space (Hafeznia,2010).

3-2.Cyber Power

The concept of cyberspace is indeed blurring traditional boundaries of the time and place. In a networked world, digital technologies enable communication and interaction that transcend physical locations and time zones. As communication technologies like the internet, social media, and virtual platforms evolve, individuals can engage with others in real-time or asynchronously, regardless of geographic constraints. Cyberspace creates a shared virtual environment where time and place become fluid concepts. For instance, individuals from different parts of the world can collaborate on projects simultaneously through platforms like Zoom or Slack, effectively negating the limitations of physical distance (Castells,2009:407). Similarly, social media platforms allow users to interact with content from various times and places, creating a continuous, interconnected stream of information (Wellman and Haythornthwaite,2002:16). In fact, cyberspace is intermingling time and place by enabling interactions that transcend traditional boundaries, leading to new forms of communication, community, and identity.

Another and important outcome of cyberspace is power. Owners of cyberspace have power and can use it for national interests. This technology

has created a new aspect of power which is effective in the equations of the international system. In terms of cyber power, this concept encompasses both the offensive and defensive capabilities a state or actor possesses in cyberspace. Offensive cyber power involves the ability to execute cyber-attacks that can damage or disable an opponent's digital infrastructure. The Stuxnet worm, discovered in 2010, is a notable example of an offensive cyber operation. This sophisticated piece of malware was designed to sabotage Iran's nuclear enrichment program by causing centrifuges to malfunction, reflecting the strategic use of cyber tools to achieve geopolitical goals (Zetter,2014:116). Defensive cyber power involves measures to protect and secure one's own digital infrastructure from cyber threats. This includes implementing robust cybersecurity practices such as network security protocols, encryption, and continuous monitoring for potential vulnerabilities. The National Institute of Standards and Technology (NIST) provides comprehensive guidelines for enhancing cybersecurity, emphasizing the need for an adaptive and resilient defense strategy to protect critical assets (NIST,2020:23).

The strategic use of cyber power also extends to influencing public perception and manipulating information. For instance, during the 2016 U.S. presidential election, Russian operatives used social media to disseminate disinformation and influence voter behavior, demonstrating how cyber power can be employed for psychological and political impact (Mueller. 2019:45).

Cyber warfare and cyber power are intertwined aspects of contemporary security dynamics. The ability to conduct and defend against cyber operations has become a fundamental element of national and international security strategies.

3-3.Geopolitics

Geopolitics is among the applied concepts that are used in political literature of today's world. But like many other things, its history is older than its formal creation in the 19th century (Malek Mohammadi,2015). the term Geopolitics was coined by Rudolf Kjellen, a Swedish scientist in 1899. Creation this term sampled definition of harsh and brutal relations. Nowadays the Geopolitics word is used in political geography, international relations, political sciences and so on. The role of geographic factors in international relations is called geopolitics. Power is decisive in geopolitics (Mojtahedzade and Asgari,2011:66). Geopolitics traditionally studies the

links between political power and geographic space, and examines strategic prescriptions based on the relative importance of land power and sea power in world history.

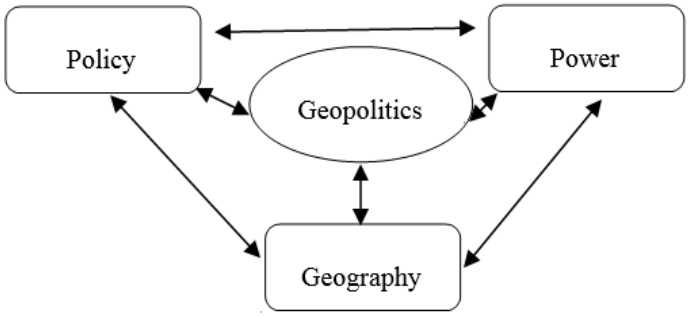

Figure (3): Conceptual Model of Geopolitics
(**Source:** Hafeznia,2006:37)

One of the foundational theories in geopolitics is the Heartland Theory, proposed by Halford Mackinder in 1904, which posits that the state controlling the central area of Eurasia, known as the Heartland could dominate global affairs (Mackinder,1904). This theory highlights the strategic importance of land-based power as opposed to maritime power.

Another key concept in geopolitics is the Rimland Theory, developed by Nicholas J Spykman in the mid-20th century. Spykman argued that the coastal fringes of Eurasia, the Rimland are crucial for controlling global power, as these regions act as a buffer between the Heartland and the world's oceans (Spykman,1944). This approach shifts the focus from central Eurasia to the surrounding territories, emphasizing the significance of controlling the peripheries.

Contemporary geopolitical analysis often incorporates critical geopolitics, which critiques traditional geopolitical theories by examining how geopolitical knowledge is constructed and used by political elites to justify power (Ó Tuathail and Dalby,1998). This approach emphasizes the subjective nature of geopolitical narratives and how they shape foreign policy decisions.

Additionally, geopolitics today must consider the impact of globalization and technological advancements. The increasing interdependence of states and the rise of cyber warfare challenge traditional geopolitical concepts that were primarily focused on physical geography.

4. Findings

4-1.Virtual Space

The concept of geography has changed and new phase of space has been shaped: virtual space. Meanwhile Space and place have been affected by new element: The Information. The information revolution has caused evolutional changes in the world. The main outcome of this forehead trend is omitting distance. The world under this evolutional change has found new form of space and place. This new form is like Marshal McLuhan's Global Village idea. The information revolution, also known as the third revolution, which the digital computer heralded 50 years ago, has profoundly changed the way society in general works and interacts.

Todays, technology, especially communications, has caused borders lose their effect in separating countries. The important feature of these types of technologies is the fast transmission of information as well as crossing international boundaries and reaching the destination in a very short period of time. The non-physical nature of communication has led to the emergence of virtual space.

Virtual spaces, often defined as computer-generated environments where users can interact with each other and the digital environment itself, have become increasingly significant in both social and professional settings. According to The Metaphysics of Virtual Reality by Michael Heim, virtual space transcends mere simulations by creating immersive environments that can mimic or even improve upon reality (Heim,1993:47). Heim argues that virtual spaces offer a new way of experiencing the world that challenges traditional notions of physicality and presence.

In a more practical context, Understanding Virtual Reality by William Sherman and Alan Craig explores how virtual spaces are utilized in fields such as education, medicine, and architecture (Sherman and Alan,2003: 214). For instance, medical professionals use virtual environments for surgical simulations, allowing for risk-free practice, which is particularly crucial for complex procedures (Sherman and Alan,2003:219). Furthermore, the rise of social virtual spaces, such as those found in online gaming or platforms like Second Life, highlights the shift in how people form and maintain relationships. As Edward Castronova notes in Synthetic Worlds: The Business and Culture of Online Games, virtual spaces create communities that are just as real and complex as those in the physical world (Castronova,2005:138). These spaces offer users the opportunity to create

avatars, explore different aspects of identity, and interact with others in ways that can sometimes be more meaningful than in-person interactions (Castronova,2005:142).

In fact, virtual spaces represent a convergence of technology, culture, and human interaction. They are reshaping how we perceive reality and what it means to be present. As these spaces continue to evolve, their impact on various aspects of life will only deepen, as highlighted by researchers across multiple disciplines.

Virtual space is a complicated and multi-dimensional space. All dimensions affect each other and accept affection from other sides. The graph No. is an imaginal portrait of virtual space drown by Artificial Intelligence. The main and notable phenomenon is connection that causes the whole space be an active system.

4-2.Geography of Virtual Space

The concept of the geography of virtual space refers to the organization, structure, and navigation of digital environments in ways that resemble the physical geography of the real world. This idea expands beyond the simple layout of websites or online platforms to encompass a wide range of virtual realms, including online games, social media networks, and the broader internet ecosystem.

Virtual spaces often mirror real-world geography in terms of topology. For example, the structure of the internet is often visualized as a network of nodes (servers or websites) connected by links (data pathways), resembling a map of cities connected by roads. This network topology affects how users navigate the virtual space, with central nodes (like major websites or platforms) acting as hubs, analogous to large cities in the real world (Castells,2001:45).

Similar to physical geography, virtual spaces have borders and boundaries, though they are less tangible. These can include the paywalls of websites, regional restrictions on content, or even the user interface of a platform, which directs how one moves through digital space. These borders influence access and interaction, creating distinct regions within the digital world that users might traverse or be excluded from, much like countries or territories in physical space (Zook and Graham,2007:114).

In addition to physical-like structures, virtual space also has its own cultural geography. Different online communities, forums or platforms develop distinct identities and cultures, often compared to different countries or

cities with unique social norms and languages. The way these virtual spaces evolve and interact can resemble the migration patterns, cultural diffusion, and even conflicts seen in the real world (Dodge and Kitchin,2001:78).

The design of user interfaces often employs spatial metaphors that draw on our understanding of physical geography. For instance, desktops mimic physical desks, and folders represent file storage systems. Virtual reality (VR) takes this even further by creating immersive spaces that users can walk through, bringing the geography of virtual space into three dimensions and making navigation akin to moving through physical environments (Rheingold,2000:129).

The geographical organization of virtual space also impacts internet governance and policy. Just as different regions have varying laws and regulations, the internet is subject to geographical boundaries like national jurisdictions. Concepts such as data sovereignty and cyber borders highlight the intersection between virtual and physical geography, where the digital actions are constrained by physical geographical regulations (Goldsmith and Wu,2006:162).

The geography of virtual space is a rich field that draws on both the metaphorical and literal parallels with physical geography. It encompasses everything from the networked structures of the internet to the cultural and social landscapes of online communities. As virtual spaces continue to grow and evolve, the interplay between physical and digital geographies will become increasingly significant, influencing both user experience and broader societal trends.

4-3.Information Geopolitics

The geopolitics of modern age has obtained some characteristics and has experienced new era. The materialization of technology, network tools, and control, today offer another concept and realm of geopolitics, which we can tittle as Techno-Geopolitics. The basic element of current and coming era of geopolitics is information. In future warfare, the struggle for information will play a central role, taking the place, perhaps, of the struggle for geographical position held in previous conflicts. Information superiority is emerging as a newly recognized and more intense, area of competition (Davis,1996:90).

Information is more important to world affairs today than at any previous point in history as a result of recent advances in data-driven technologies. These advances have revolutionized each of the four key facets of

information power: to influence the political and economic environment of other actors; to create economic growth and wealth; to enable a decision-making edge over competitors; and to communicate quickly and securely (Rosenbach and Mansted,2019:2). Information Geopolitics is a key term to illustrate the rule of information in relation of powers. This is clear that from 1899 till now the source of power has changed. Today information is one of the main sources of power. The biggest commercial success stories of the Information Age—Alphabet (Google's parent), Facebook, Amazon, Alibaba, and Tencent—are monopolists. One explanation for this is that access to data tends to be a virtuous cycle: more data lets companies build better applications and technologies, which accelerates their profitability and popularity, and in turn ability to harvest and use even more data (Rosenbach and Mansted,2019:6).

For the first time, cybernetic was applied in military conflict in 2008, when Georgia and Russia were involved in a conflict and started to use cyber capabilities. Russia combined its military operations with cyber capabilities to increase its strategic advantage against a vulnerable Georgia. It was coordinated at the state level against another state and had far reaching consequences. Georgia's network was compromised and its cyber capabilities were limited so that a response could not be launched. This operation had its base in geopolitics because the locations of the events were chosen according to virtual locality and then were followed into the physical realm by the military (Bordelon,2016:8). One of the most important points of analysis regarding geopolitics is the possible response either to a cyber or counter-cyber-attack and how a particular measure will be perceived. Rearticulated: What kind of a response can be expected in the face of a cyber threat or during an actual attack? Given the range of responses stated earlier, national decision makers must assess how nation-states will react; for that reason, geopolitics highlights the importance of understanding both actual responses and reactions to those responses (Guiora,2017:35).

The concept of the geopolitics of information refers to the strategic control and manipulation of information in global power dynamics. In the digital age, information has become a key resource, akin to oil or military power in previous eras. Nations and corporations now vie for dominance over data flows, communication networks and the narrative control in media, recognizing that whoever controls information wields significant power on the global stage. This shift is evident in the increasing efforts by states to

control digital infrastructure and the internet. For example, China's Great Firewall exemplifies a state-driven model of information control, where the government regulates access to information and censors' content to maintain internal stability and promote its geopolitical interests (Morozov,2011:87). Similarly, Russia's approach, often termed sovereign internet, seeks to create a national internet that is insulated from global networks, thereby enabling the state to control information flows within its borders (Deibert. 2013:29). On the other hand, the United States and its allies promote a more open model, but this too is not free from geopolitical motivations. The dominance of American tech giants like Google, Facebook, and Amazon in global digital markets allows the U.S. significant soft power, influencing global norms, and the flow of information (Nye,2004:31). This also raises concerns about data sovereignty and the potential for these corporations to act as instruments of U.S. foreign policy, especially in the context of global surveillance practices revealed by the Snowden leaks (Greenwald,2014:46). The geopolitics of information thus underscores the complex interplay between state power, corporate interests, and technological infrastructure in the 21st century. As information continues to grow as a strategic resource, conflicts over its control are likely to intensify, shaping the future of international relations.

The geopolitical function of information can be realized in the following formats:

A) **Virtual Geopolitics Versus Genuine Geopolitics**

Virtual geopolitics, encompassing digital diplomacy, cyber warfare, and online influence operations, increasingly intersects with traditional geopolitical strategies. This synergy highlights how virtual realms are shaping and reflecting global power dynamics.

Virtual geopolitics involves the use of digital platforms for strategic influence and control. For instance, countries now employ cyber capabilities to conduct espionage, disrupt infrastructure, and influence political processes globally (Libicki,2012). The 2016 U.S. presidential election, influenced by Russian disinformation campaigns on social media, exemplifies how virtual tools can impact genuine geopolitical outcomes (Mueller,2019).

The interaction between virtual and genuine geopolitics is bidirectional. On one hand, virtual platforms enhance traditional geopolitical strategies by providing new tools for information warfare and diplomatic outreach. On

the other hand, geopolitical conflicts often spill into the virtual domain, where cyber-attacks and online propaganda reflect and amplify real-world tensions (Singer and Friedman,2014).

This convergence underscores the need for integrated strategies that address both physical and digital arenas. Understanding how virtual actions can influence geopolitical stability and how geopolitical conflicts can manifest online is crucial for contemporary statecraft and international relations. The assassination of Ismail Haniyeh, the explosion of pagers, and the assassination of Seyyed Hassan Nasrallah were definitely by taking advantage of these capabilities. Although it seems that Israel is vulnerable in the ground battle. The reason for its success in its recent attacks was the use of cyberspace, artificial intelligence, communication networks and firepower. Israel has carefully planned to reach such a situation.

B) Information Warfare

This form of conflict centers on the control, manipulation, and dissemination of information to influence public perception, destabilize governments or achieve strategic advantages in conflicts. Unlike conventional warfare, where the objectives are tangible and the actors are clearly defined, the war of information is characterized by its intangibility and the covert nature of its combatants. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. The war of information resembles the war of attrition. However, there are two key differences: first, in a war of attrition, both players bear costs as long as the game continues while in a war of information only one player incurs a cost at each moment. Second, the resources spent during a war of information generate a pay-off relevant signal (Gul and Pesendorfer,2011).

Because of the reason for their importance and their semantic connection, there are four types of information wars: Electronic warfare, Cyber warfare, Command Control, Computer and Communication Warfare and Psychological Warfare (Rostami,2016).

The concept of information warfare in its modern systematic framework was created in 1975. The geopolitical role of information has been applied from the Balkan war in 1990s and from that time it is expanding rapidly. Today, wars are based on information. The global battle in the 21st century is in the field of information. Information war means; The use of electronic networks

to destroy or disable and make non-operational the enemy's information infrastructure, which can be used against a society as well as against the army or military force of a country (Ahmadiyaghin,2022).

The consequences of information warfare are far-reaching, affecting not only military operations but also political stability and social cohesion. As governments and organizations become increasingly aware of the threats posed by information warfare, they are developing new strategies and technologies to defend against these attacks. However, the rapidly evolving nature of this domain means that the war of information is likely to remain a significant challenge in the years to come.

C) Cyber Attacks

Transitioning from traditional warfare to cyberterrorism and cyber warfare reflects a significant change in the nature of conflict and modes and manners of defense. If traditional warfare between nation-states involved tanks, planes, and ships, then cyber-attacks, whether conducted by nation-states or nonstate actors, require a laptop and computer sophistication and savvy. Cyber-attacks address nation-state infrastructure but can also address infrastructure moving forward (Guiora,2017:16).

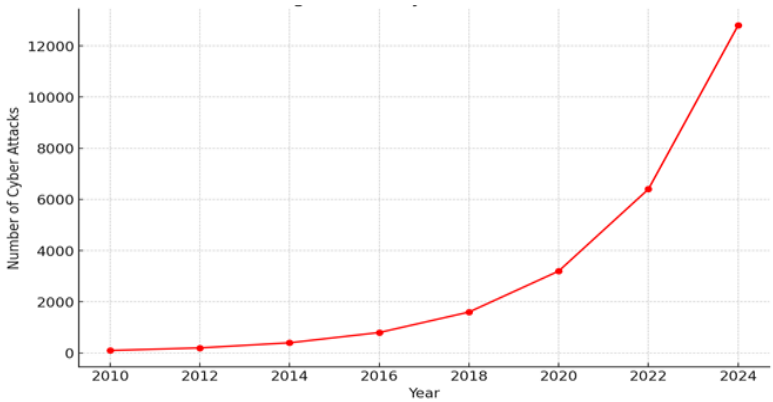

Figure (3): Increasing Trend of Cyber Attacks over Time

(**Source:** Statista.com)

States have access to new means of attack and espionage through cyber systems that were not available in the previous decades. Non-state actors, such as private individuals, also have access to cyberspace (Bordelon,2016: 5). The USA as the main super power in this arena has control over the main bases. The technical and technological management of the global network, the Internet, in the form of the ICANN company, although private, but with

an American identity, exists in California. The root and basic servers of the Internet network and the management of the majority of memory servers in this network are located in the United States, or their management and control are in the hands of the main companies based in the United States, such as Yahoo, Google, Microsoft, Facebook, YouTube, HP, Twitter and so on (Hafeznia,2010).

Table (1): Share of Attacks by Industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and Insurance	18.2%	18.9	22.4	23	17
Professional, Business and Consumer Services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and Wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and Telecommunications	1.2%	0.5	2.5	5.7	10

(**Source:** IBM,2024:46)

The geopolitics of cybernetics refers to the strategic and political implications of the integration of cybernetic systems—those involving human, machine, and networked interactions—into the global power landscape. This concept encompasses the ways nations leverage cybernetics, including artificial intelligence, autonomous systems, and information networks, to exert influence, protect sovereignty, and gain competitive advantages. Through remote sensing and GIS, the amount of error is reduced and the achievement of the goal is guaranteed to a large extent. The pager explosions of Lebanon's Hezbollah is the newest one of this kind of cyber-attacks that took place. Citing US officials, the New York Times said that the pagers received messages that appeared to be coming from Hezbollah's leadership before detonating. The messages instead appeared to trigger the devices, the outlet reported (BBC,September 2024).

D) Role of Artificial Intelligence in Geopolitics of Information

Artificial intelligence (AI) has dramatically transformed the landscape of cyber-attacks, introducing both sophisticated offensive capabilities and enhanced defense mechanisms. AI's role in cyber warfare has evolved from simple automation to complex, autonomous systems that can identify

vulnerabilities, launch attacks, and even adapt in real-time. One of the primary ways AI enhances cyber-attacks is through the automation of malicious activities (Fruhlinger,2023). AI-driven tools can quickly analyze vast amounts of data to discover security weaknesses in software or systems. This capability enables adversaries to launch more precise and effective attacks. For example, AI can be used to create advanced phishing schemes, where machine learning algorithms craft highly personalized emails that are more likely to deceive recipients into disclosing sensitive information or installing malware (Fruhlinger,2023).

Additionally, AI enables the development of sophisticated malware that can adapt to evade detection. Traditional malware is often designed with fixed behaviors, but AI-powered malware can modify its tactics based on the responses it receives from security systems. This makes it harder for conventional antivirus programs to detect and neutralize such threats. Researchers have demonstrated how AI can generate polymorphic code that changes its structure to avoid detection by static analysis tools.

AI is also playing a crucial role in amplifying denial-of-service (DoS) attacks. Machine learning algorithms can optimize the distribution of attack traffic, making it more challenging for defenders to mitigate the impact. For instance, AI can orchestrate massive botnet attacks that are capable of overwhelming even the most resilient networks (Shackleford,2022).

However, the use of AI in cyber-attacks also highlights the growing need for AI-driven cybersecurity defenses. Just as AI enhances offensive capabilities, it also offers tools for more effective threat detection and response. AI systems can analyze patterns and anomalies in network traffic, predict potential vulnerabilities, and respond to threats in real-time. This dual-edged nature of AI underscores the importance of ongoing research and development in both offensive and defensive cyber technologies (Sanger and Perlroth. 2023). Yashuva Bengio who is called the Godfather of AI in an interview with yahoo finance in October 11, 2024 said: Intelligence gives power, and whoever controls that power — if it's human level or above — is going to be very, very powerful,"(finanace.yahoo.com).

The global AI budget and investment landscape is led by the United States and China, with the U.S. having invested approximately 249 billion dollars in AI since 2013. China follows with 95 billion dollars in AI investments over the same period. The UK ranks third with 18 billion in AI investments, while other notable countries include Israel 11 billion, Canada 9 billion and

France 7 billion dollars. In 2022 alone, U.S. AI startups raised 47 billion, while China's AI startups attracted 71 million on average per company. The sectors receiving the highest AI investments globally include healthcare 6.1 billion, data management 5.9 billion, fintech 5.5 billion and cybersecurity 5.4 billion dollars (IDC.com).

In terms of funding, the U.S. is massively ahead, with private AI investment totaling 335 billion dollar between 2013 to 2023. AI startups in China raised 104 billion over the same timeframe, while those in the UK raised 22 billion dollars. Further analysis reveals that the U.S. is widening this gap even more. In 2023, for example, private investment in the U.S. grew by 22% from 2022 levels. Meanwhile, investment fell in China (-44%) and the UK (-14.1%) over the same time span(visualcapitalist.com).

E) Cyber Security

Along with the ease of establishing communication, some vandalism has emerged. In other words, as much as it is useful and practical, virtual space can be equally destructive and cause a lot of damage to a country. The fragility of cyberspace exists everywhere, but in developing and underdeveloped countries, this fragility is costly and damaging.

The issue of information and communications technologies (ICTs) in international security has been on the UN agenda since 1998, when Russia first proposed a cyber arms control treaty (Ruhl and Others,2020:5). Cybersecurity has become a global problem, whether viewed in economic, humanitarian, or national security terms. In economic terms, the 2017 WannaCry ransomware infected hundreds of thousands of computer networks in 150 countries, with losses totaling up to 4 billion dollars. The White House estimated that the total damages from NotPetya reached 10 billion dollars. According to the U.S. Council of Economic Advisers, malicious cyber activity caused between 56 and 109 billion worth of damage to the U.S. economy in 2016 alone (Ruhl and Others,2020:2).

Nation-state cyber risk arises from the objective for certain countries to establish dominance over their adversaries. This includes the development of offensive capabilities that allow one country to target the assets and infrastructure of an adversary. Such offenses usually stem directly from the military, which implies that the capabilities are advanced and effective. Cybersecurity, on the other hand, is a critical component of national security as the digital landscape becomes a battlefield of its own. Importantly, cybersecurity can no longer be considered merely a technical issue, but has

spilled over to the geopolitical realm. Cyberspace is becoming the new battleground for states to jostle for control over such critical technologies and to set the agenda for technical standards globally. Cyber capabilities and critical technologies are shaping up as tools of state power that can be used against adversaries (Koh,2020). Today, with the rapid and extensive expansion of the Internet and the growth of the digitization process of industries, Services and infrastructures, geopolitics gets more and more far from its geographical basis and intertwined with virtual realities (Ahmadi, 2023).

4-4.Cyber Wars and Conventional Wars

Interactions among individual actors in a global cyberspace create a fundamental stipulation for international security. In this connection, it can be claimed that all technical equipment that produce the simulated illusory projection of intersubjective virtual online spaces can be considered as hard power component for smart virtual power. The virtuality construction as a product may be distributed via technological equipment within a particular geographic area or an institutional matrix zone and influence individuals` behavior strategies, their economic preferences and cultural values (Lobastova,2020).

currently the distribution of technological equipment on the surface of the Earth is not equal. The absence of digital equipment within geographical territory signals the impossibility to distribute the information. Consequently, the global cyberspace could serve a platform for hegemony extension of the governing elites. Ideological center can be represented not only by national government departments, but also by nonstate actors that have a political significance on the international stage. Globally spread networking systems have influenced the essential processes of humanity existence on micro and macro levels. They also synchronize basic human life processes across geographical boundaries, time zones and cultural prejudices. Social relations have already been hybridized into offline and online environments both (Lobastova,2020).

Cyberspace is different from real space. The first disparity is environment. Both of them have their own environment and elements and so agents of war are different in both environments. Agents of war in cyberspace are sabotage commands sent under the title of a special program, which is usually known as a virous and worm and is a software command to disrupt

financial, military, nuclear, administrative, service, infrastructure, health, security systems and so on.

In the real space, natural obstacles (time, place and weather conditions) play an important role in delaying the operations but in cyberspace operations, natural obstacles do not play a substantial role. The amount of destruction of the operations in the real war depends on the amount of force and the volume of fire and but in the cyber war, it may not necessarily be a war operation and have no human casualties. Cyber wars often happen in a cyber environment, so type of attack is different in two wars. Real wars can be started by anyone, but the finisher is the powerful side, but cyber war is started only by those who have the ability and technology. Real war may take a long time and ammunition and military force are constantly needed, but cyber war works like lightning and causes damage to the enemy in an instant.

The very important difference between today's technology-based wars and the past wars is that the financial and human cost of technology-based wars in a short period of time is much higher than the past wars. In other words, in modern wars, significant human and financial losses are imposed on the enemy in a short period of time. The casualties of modern wars do not necessarily end with human deaths, but can target financial and health institutions, etc., which will impose a huge cost on the enemy. The advancement of technologies has paved the way to emerge of more devastating wars, and this is inevitable. Offenses have taken a new form in the new era, so the defenses must also have the necessary preparation to deal with them. And as the final words: cyberspace has become a new realm of geopolitical conflicts. Countries in this new realm will be more successful if they have more and better technological capabilities to attack and defend.

The most important limitation of cyber warfare is the lack of network, power outages or internet network outages.

Table (2): Genuine Space and Cyberspace in Comparison

Indicatrs	**Genuine Space**	**Cyberspace**
Environment	Real	Virtual
Toll, Casualty	Man and his Belongings	Mostly Infrastructures
Operation and Reaction	Normal	Immediate
Natural Obstacles	Effective	Ineffective
Vulnerability	Shortage of Ammunition and Forces	Network DC

Cyber warfare and cyber power are critical components of modern conflict and national security. Cyber warfare involves the use of digital attacks by one nation-state or actor to undermine the capabilities, stability, or security of another. These attacks can target critical infrastructure, disrupt communications, and compromise sensitive data. A prominent example of cyber warfare is the 2007 cyberattack on Estonia. Over several weeks, a series of distributed denial-of-service (DDoS) attacks overwhelmed Estonian government websites, financial institutions, and media outlets, demonstrating the potential for cyber operations to disrupt a nation's functionality and societal stability (Zetter,2014:85). This attack was attributed to Russian cyber actors, highlighting the use of cyber capabilities for geopolitical purposes.

The efficiency of virtual and cyberspace and the increase of its capabilities have made cyber power to be defined as a new dimension of power. Countries with cyber power have the upper hand in defeating the enemy. nowadays Cyber wars are expanding because attacking on various infrastructures causes a lot of damage to the enemy. hence cyber power and cyber attacks are an important challenge in geopolitical issues.

5. Conclusion

The world has entered a new phase in the third wave of the information revolution, where everything is changing. The scope of these evolutionary changes is vast and far-reaching, with technology experiencing significant and profound changes at a rapid pace. One of the key outcomes of the modern era is the diminishing role of geographical distance. Essentially, in the third millennium, geography has undergone a significant transformation by eliminating or reducing the impact of distance, primarily due to technological advancements in the virtual space.

Virtual space emerged with the birth of the Internet and has since expanded greatly, proving its effectiveness and becoming widely used worldwide. The key to success lies in adapting to new technological conditions. As a result, the wave of transformation has extended to cyberspace, providing it with the tools necessary to harness power. The integration of time and space has unveiled a new dimension of power, showcasing the role of new technologies in espionage, surveillance, and military operations, and their ability to serve the interests of nations. In the traditional approach to these issues, tools were primarily physical, but the capabilities of modern

technologies have shifted the focus away from physical agents to technology, thus replacing the human role with advanced tools.

Cybernetics has become a key domain in international relations, as nations increasingly rely on digital infrastructures and AI-driven systems for economic growth, military operations, and governance. Control and development of these technologies have led to a new form of geopolitical competition, where nations vie for supremacy in the digital and technological realms. For instance, the United States and China are often seen as leading powers in the race for Artificial Intelligence dominance. Both countries invest heavily in AI research and development, considering it crucial for maintaining or achieving global superpower status. This competition is often referred to as the AI arms race, where advancements in AI are seen as critical to national security, economic leadership, and international influence.

Nowadays countries view their cybernetic infrastructure—encompassing networks, data centers, and AI systems—as vital national assets. The protection of these assets from cyber-attacks, espionage, and sabotage is a top priority. The geopolitical landscape has thus expanded to include cyberspace as a new ground of conflicts, where cyber-attacks can be as damaging as physical attacks. The Stuxnet attack on Iran's nuclear facilities in 2010, widely attributed to the United States and Israel, demonstrated the potential of cyber-attacks to achieve geopolitical objectives without traditional military intervention. This has led to the development of national cyber defense strategies and the establishment of cyber commands within military organizations worldwide.

AI and autonomous systems are impacting the geopolitical order by altering the nature of warfare, governance, and economic competition. Autonomous weapons, for instance, pose ethical and strategic concerns as they have the potential to reduce the threshold for conflict and alter power dynamics. In the economic sphere, AI-powered innovation plays a crucial role in determining national competitiveness.

As technology advances, the geopolitics of cybernetics will grow increasingly intricate. Emerging technologies like quantum computing, 5G networks, and the Internet of Things (IoT) will add new layers to this geopolitical landscape. Countries will need to navigate these challenges by striking a balance between reaping the benefits of technological progress

and addressing security, ethical, and international cooperation considerations.

The developments in cyberspace and its integration into power relations have given rise to a new dimension of power. This new dimension is primarily held by countries with the necessary software and hardware capabilities in the field of cyberspace technologies. The effectiveness of these new technologies has been demonstrated in recent conflicts. According to the findings of the article, this new dimension of power has moved beyond the testing phase and is now in the functional proof stage, having achieved significant successes on the battlefield. It is evident that cyber power is now a crucial aspect of power in the current realistic world. These new technologies have increased the likelihood of achieving victory over the enemy.

References

1. Ahmadi, B. (2023). "Emerging cyber geopolitics; an opportunity for convergence in the Persian Gulf" Scientific Journal Quarterly of Middle East Studies, Vol 29. No 4. Pp: 1-13. **[In Persian]**
2. Ahmadiyaghin, M. (2022). "The Role of Geopolitics of Information in the Design of Modern Combat Strategy with Emphasis on Complexity-Chaos Theory" Journal of Geography, Vol.20, No.72, PP: 113-135. **[In Persian]**
3. Bordelon, E.B. (2016). Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law, A Senior Thesis submitted in partial fulfillment. Liberty University.
4. Castronova, E. (2005). Synthetic Worlds: The Business and Culture of Online Games. University of Chicago Press.
5. Castells, M. (2009). The Rise of the Network Society. Blackwell Publishers.
6. Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press.
7. Davis, N.C. (1996). AN INFORMATION-BASED REVOLUTION IN MILITARY AFFAIRS: In Athena's Camp. John Arquilla and David Ronfeldt Published by RAND Corporation.
8. Deibert, R. (2013). Black Code: Inside the Battle for Cyberspace. Signal.
9. Dodge, M; Kitchin, R. (2001). Atlas of Cyberspace. Addison Wesley.
10. Rheingold, H. (2000). The Virtual Community: Homesteading on the Electronic Frontier. MIT Press.
11. Fruhlinger, J. (2023). "How AI is Making Cyberattacks More Dangerous." CIO. Retrieved from https://www.cio.com/article/362108/how-ai-is-making-cyber-attacks-more-dangerous.html.
12. Gleick, J. (2011). The information: A history, a theory, a flood. Pantheon Books.
13. Goldsmith, J; Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.
14. Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books.
15. Guiora, A.N. (2017). CYBERSECURITY, Geopolitics, Law and Policy. Routledge, London.
16. Gul, F; Pesendorfer, W. (2011) "The War of Information" Review of Economic Studies, No. 79, PP: 707-734.
17. Isaacson, W. (2014). The innovators: How a group of hackers, geniuses, and geeks created the digital revolution. Simon & Schuster.
18. Hafeznia, M.R. (2006). Principles and Concepts of Geopolitics. Mashhad, Papoli Publications. **[In Persian]**
19. Hafeznia, M.R. (2010). "Geopolitical conceptualization of internet and virtual space" Geopolitics quarterly, Volume 7, No. 1, PP: 1-13. **[In Persian]**
20. Heim, M. (1993). The Metaphysics of Virtual Reality. Oxford University Press.
21. IBM (2024). X-Force Threat Intelligence Index 2024 .

22. Koh, D. (2020). The Geopolitics of Cybersecurity. The Diplomat, 9 December .
23. Kello, L. (2017). "The Virtual Weapon and International Order" Yale University Press, pp. 98-112.
24. Kitchin, R; Dodge, M. (2011). Code/Space: Software and Everyday Life. MIT Press.
25. Goldsmith, J Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.
26. Libicki, M.C. (2012). Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.
27. Leiner, B.M; Cerf, V.G; Clark, D.D; Kahn, R.E; Kleinrock, L; Lynch, D.C; ...; Wolff, S. (2009). "A brief history of the internet" ACM SIGCOMM Computer Communication Review, 39(5), 22-31.
28. Lobastova, S. (2020). "Geopolitics of Cyberspace and Virtual Power" Journal of Liberal Arts and Humanities (JLAH) Issue: Vol. 1; No. 3, PP: 97-113.
29. Mackinder, H.J. (1904). "The Geographical Pivot of History" The Geographical Journal, 23(4), Pp: 421-437.
30. Malek Mohammadi, H. (2015). "Techno-Geopolitics; a pro classical geopolitics challenging critical approach, Geopolitics Quarterly" Volume: 10, No 4, PP: 109-121. **[In Persian]**
31. Mueller, R. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice.
32. Mojtahedzadeh, P; Asgari, S. (2011). Political Geography and Geopolitics, Payam Noor University, Tehran, Iran. **[In Persian]**
33. Morozov, E. (2011). The Net Delusion: The Dark Side of Internet Freedom. Public Affairs.
34. National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity. NIST.
35. Nye, J.S. (2004). Soft Power: The Means to Success in World Politics. Public Affairs.
36. Nye, J. (2010). "Cyber Power and National Security" Harvard University Press, Pp. 125-130.
37. Ralston, A; Reilly, E.D; Hemmendinger, D. (2003). Encyclopedia of Computer Science. John Wiley & Sons .
38. 38-Clarke, R.A; Knake, R.K (2010). Cyber War: The Next Threat to National Security and What to Do about It, Harper Collins, New York.
39. Clarke, R.A; Knake, R.K (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Penguin Press .
40. Rosenbach, E; Mansted, M. (2019). The Geopolitics of Information, Harvard Kennedy School, Belfer Center for Science and International Affairs .
41. Rostami, F. (2016). "Changes in the nature of future wars, the Islamic Republic of Iran, Scenarios, opportunities and challenges" Defense Policy Journal, No. 97, Pp. 145-190. **[In Persian]**
42. Ruhl, Ch. and Others, (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads, CARNEGIE ENDOWMENT FOR

INTERNATIONAL PEACE.
43. Shackleford, S. (2022) "AI in Cyber Warfare: How AI is Revolutionizing Cyber Attacks. CSO Online" Retrieved from https://www.csoonline.com/article/ 3536282/ ai-in-cyber-warfare-how-ai-is-revolutionizing-cyber-attacks.html.
44. Sherman, W; Alan C. (2003). Understanding Virtual Reality: Interface, Application, and Design. Morgan Kaufmann .
45. Sanger, D.E; Perlroth, N. (2023). "The New Cyberwarfare Threat: AI-Powered Malware" The New York Times. Retrieved from https://www.nytimes.com/ 2023/05/21/technology/ai-cyberwarfare.html.
46. Singer, P.W; Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press.
47. Spykman, N.J. (1944). The Geography of the Peace. Harcourt, Brace and Company.
48. Ó Tuathail, G; Dalby, S. (1998). Rethinking Geopolitics. Routledge.
49. Wellman, B; Haythornthwaite, C. (2002). The Internet in Everyday Life. Wiley-Blackwell.
50. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.
51. Zook, M; Graham, M. (2007). "The Creative Reconstruction of the Internet: Google and the privatization of cyberspace and DigiPlace" Global Networks, 38(6), Pp: 1322-1343.
52. https://www.livescience.com/20718-computer-history.html.
53. https://www.statista.com/statistics/617136/digital-population-worldwide/.
54. https://www.techtarget.com/searchnetworking/answer/What-are-the-3-most-common-network-issues-to-troubleshoot.
55. https://www.anonymoushackers.net/cybersecurity-news/countries-with-the-best-hackers-in-the-world-2023/.
56. https://www.bbc.com/news/articles/cz04m913m49o.
57. https://www.idc.com/getdoc.jsp?containerId=IDC_P33198.
58. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.
59. https://www.visualcapitalist.com/mapped-the-number-of-ai-startups-by-country/.
60. https://finance.yahoo.com/news/ai-godfather-yoshua-bengio-were-creating-monsters-more-powerful-than-us-120042014.html.