

Cyberspace, Cyber Power, and Digital Sovereignty: A Geo-Strategic Analysis in the Era of Digital Transformation

Mounira BOUDERDABENE ^{1*}, Mounir LIMANE ²

¹ University of Constantine 3 Salah Boubnider, (Algeria).

mounira.bouderdabene@univ-constantine3.dz

² University of Msila, (Algeria), mounir.limane@univ-constantine3.dz

Date of submission: 25/03/2026

Date of acceptance 19/05/2026

Date of publication: 11/06/2026

Abstract:

This paper examines the geostrategic nature of cyberspace as an extension of traditional rivalries and conflicts across land, sea, air, and space domains, emphasizing digital sovereignty as a cornerstone of cybersecurity defense strategies. It is structured around three key axes: first, the characteristics of cyberspace as a contested military domain where cyber warfare and espionage amplify power through control; second, the concept of digital sovereignty illustrated by Russia's localization of data storage centers to counter U.S. dominance and reduce vulnerabilities; third, the challenges of rapid digital transformation, which expands attack surfaces via cloud computing, artificial intelligence, and the Internet of Things (IoT), necessitating flexible strategies that blend proactive defense with counter-offensive measures while balancing sovereignty and freedoms. The study concludes that bolstering security doctrine through digital sovereignty is essential to address multidimensional threats in the digital transformation era.

Keywords: Cyberspace; Cyber Power; Digital Sovereignty; Geo-Strategic Analysis; Digital Transformation.

* Corresponding author.

1. Introduction

Over the past two decades, cyberspace has become one of the most significant geopolitical issues for states. Ongoing cyberattacks against state interests and various economic enterprises by both state and non-state actors have made this a contentious space, as indicated by the terms used in this field: ‘cyber battles’, ‘cyber wars’, ‘cyberattacks’, ‘cyber espionage’, and so on. This is a characteristic shared with the traditional dimensions of state territory: land, air and sea. These terms emphasise that cyberspace is a realm of strategic activity and that its importance to states and non-state actors is continuously increasing.

However, we should not view the growing importance of cyberspace as a revolutionary change that has completely transformed patterns of international competition and conflict. Rather, we must understand this space’s significance within a framework indicating that it is an extension of international competition and conflict in a new fourth dimension — cyber space — or a fifth dimension, after land, air, sea and outer space. In other words, cyberspace provides an opportunity for forms of competition, conflict and strategic activity to emerge that are not entirely new, but which have previously existed within the traditional territories of states. Furthermore, cyberspace is closely linked to the physical territory of states and subject to the same pathways and dynamics that govern issues of sovereignty and power within a state.

From this reading, we understand that cyberspace is not entirely independent of the geographical reality of states and their geopolitical interests. Its primary truth is geographical, as it is linked to the territories of states. Secondly, it is a domain subject to calculations of sovereignty and power (authority) within the state, making it geopolitical. The issue of undersea cables, for example, which form the main component of the physical communication network and are essential for the existence of cyberspace, is fundamentally linked to geography. This geographical reality creates advantages for some states and challenges for others, making it a source of strength or weakness for states.

Thus, the most important lesson we can conclude from the two readings above is that cyberspace is fundamentally a geo-strategic space. Breaking down this phrase reveals that

- 1) it has a geographical dimension involving sovereignty issues and
- 2) it is also a domain of strategic activity for states. In this sense, it is a

space that poses threats to states and their various interests and provides a justification for intervention and securitisation.

This paper explores the conceptual and doctrinal aspects that could be incorporated into potential strategic frameworks on this issue. It will address the following question:

how has cyberspace become a source of threats from another dimension, extending its traditional conflicts? How can the characteristics of these threats be incorporated into cybersecurity defence strategy?

This study is based on the assumption that, cyberspace and the threats within it represent an extension of its traditional conflicts. Therefore, it is a fourth dimension of territory that should be subject to an understanding of sovereignty that allows for the greater securitisation of essential national interests.

In order to analyse this issue, we will address three elements in order to demonstrate that the foundational components of a cybersecurity defence strategy for states should revolve around the concept of digital sovereignty. This approach aims to support and strengthen states' defensive security doctrine by combining defensive tactics with various high-level threats to security and the necessity of employing offensive (disruptive) tactics.

The first element will focus on identifying the fundamental characteristics of cyberspace from a theoretical perspective. This will enable us to understand the security challenges and threats states face in this context.

The second element will analyse the defensive measures that some countries have adopted within this framework, revealing the importance of digital sovereignty as a core component of a cybersecurity defence strategy.

The third element will address global digital transformation and the security challenges it poses at defence and military levels. It will examine how components for formulating a global response are still in development. This indicates the potential to direct these responses towards a vision oriented towards sovereignty and protection, as well as a more militarised approach of states' defensive efforts in the cybersecurity domain.

2. The Concept of Cyberspace: A Geo-Strategic Approach

The term 'cyberspace' originated in science fiction, referring to a virtual world where the qualifier 'virtual' symbolises detachment from reality. This connotation can also extend to the field of political science, as the term may

suggest to many readers — including specialists — that it is a non-territorial space, meaning it is not linked to a specific geography or framed by the sovereignty of any state. However, this interpretation is a conceptual fallacy due to its ambiguity and semantic inaccuracies. This definition has now been abandoned, with cyberspace being viewed as an ‘extension of social reality and a space of work and activity in which all social functions are performed’ (Warusfel, 2021).

Based on this concept, we will see that it is essential, from a security perspective, to establish a framework for understanding cyberspace as a field of strategic and military activity.

2.1. Cyberspace as a Military Space

According to researcher Olivier Kempf, the term ‘cyberspace’ is primarily geopolitical and military. According to Kempf, the first argument for this stems from the meaning of the word ‘cyber’ itself, which denotes ‘skill and proficiency in movement’. The term ‘cybernetics’ was first used by the physicist Ampère in 1834 to mean ‘the art of managing and governing individuals’. After 1945, it began to refer to the field of controlling communication processes (Kempf, 2012).

Today, the term ‘cyber’ has a purely technical connotation, referring to computers and their networks. The realm in which these networks extend is known as cyberspace (Baur-Ahrens, 2017). The term was first coined by novelist William Gibson in his 1984 work *Neuromancer* (Ventre, 2011). The concept gained popularity during the 1990s and is now the subject of study and research in most social science and artificial intelligence fields.

Thus, the concept of cyberspace refers to that virtual—yet also material and abstract—realm in which information flows between an infinite number of interconnected computers (Kempf, 2012). This definition should not suggest that cyberspace is merely a virtual space isolated from the material and geographical realities of the territory under the sovereignty of a state; rather, it must be understood in completely opposite terms to this initial perception.

The theory of the three layers addresses this issue by asserting that:

- 1) this space is primarily a geographic reality.
- 2) it becomes a space for conflict and confrontation when the constraints, procedures and activities occurring within it affect the security and interests of the state. The theory illustrates that cyberspace comprises three layers.

1. The Physical Layer: This includes computers and communication infrastructures, which are essential for the existence of a virtual world. This layer is inherently geographic and territorialised.

2. The logical layer (software): This refers to the interconnectivity provided by protocols, codes and software. Without the ability to communicate with each other, these computers and infrastructures hold no meaning.

3. The semantic layer (la couche sémantique ou informationnelle): This layer encompasses the content, data and information transmitted and exchanged. It is fundamentally about the content itself (Kempf, 2012, p. 123).

According to Daniel Foneur, these layers are interconnected through three levels:

- 1) a physical level based on equipment;
- 2) a level comprising the platforms designated for accessing this space; and
- 3) a level of media connectivity across networks (Ventre, 2011).

Therefore, it should be noted that cyberspace is not merely a technical concept or virtual construct as portrayed in science fiction, but rather a system of interconnected networks and a means of moving information, forming a two-dimensional space comprising a social dimension and a cognitive dimension.

Historically, the geopolitical and geo-strategic reality of cyberspace did not begin until the 1990s in the United States (Gagnon & Rapin, 2021). It was not until the beginning of the current millennium that official military interest in the geostrategic dimensions of this space materialised, thus revolutionising military affairs by adding a fifth dimension to conflict (in addition to land, sea, air and space).

Military doctrinal documents from various major countries now explicitly refer to cyberspace as an operational domain. In the US, the Department of Defense adopted its first 'National Strategy for Operations in Cyberspace' in 2006, emphasising that cyberspace primarily serves as

- 1) a domain for intelligence
- 2) a space for influencing foreign public opinion and other nations (Baur-Ahrens, 2017). In France, the 2008 White Paper on Defence and Security pointed to the dimensions of 'attacks and conflicts in the computing field'.

A significant qualitative shift occurred in 2009 when U.S. military

documents, specifically the ‘Joint Capability Areas’, defined cyberspace as ‘a distinct and unique environment comprising four components: cyber warfare, cyber network operations, cyber support, and cyber reconnaissance and information operations’¹.

2.2. Cyberspace as a Contested Space and a Space of Power

Through the various operations conducted by different states and the vocabulary that has emerged in this context, we have seen how cyberspace has also become a military concept. This includes terms such as ‘cyber warfare’, ‘cyberattacks’ and ‘cyber espionage’, all of which carry military connotations. While the concept of cyber warfare is perhaps the most powerful, its ability to provide a sound scientific understanding of cyberspace is limited to utilitarian purposes, and its explanatory power is relatively weak².

Therefore, in our attempt to strengthen our understanding of the strategic dimensions of cyberspace, we propose that these terms represent various aspects, forms and tactics of a broader concept: conflict. The advantage of this approach is that it enables us to broaden our focus beyond concepts of war and attacks, recognising them as mere means and tools within larger, more comprehensive dynamics of power and resulting conflicts. It also enables us to assert that, with its wars and conflicts, cyberspace is another arena for power relations and disputes, extending these dynamics beyond traditional state territories (land, sea, air and space).

It is therefore pertinent to examine the tools and factors of power at the cyber level.

A. Cyber warfare as a tool of power in cyberspace

The concept of cyber warfare, reflecting one of the most significant forms of conflict between states, deserves attention here. However, it should be considered in the context of the digital space as a domain of power. Cyber warfare operations are defined as military operations that target an adversary’s or enemy’s interests

¹ The first official address in the United States regarding the dangers of cyberspace dates back to 1995. However, conflict and security issues only began to be included in the discourse surrounding cyberspace security in the early 2000s. For more details, see: (Baur-Ahrens, 2017).

² In this field, we prefer to use the concepts of cyber conflict or digital conflict instead of terms such as war, attacks and espionage, as these carry purely military connotations and are rooted solely in legal considerations. Therefore, we believe that these concepts often fail to accurately reflect the reality of cyberspace. For example, if country A launches an electronic attack against country B, is this considered a military and legal act of war? There is no definitive answer; this action can be classified as both hostile and competitive behaviour. However, to date, no country has considered such behaviour to be an act of war. Therefore, we prefer to use the concept of cyber conflict, as this accommodates all these forms and contentious methods. Further details can be found in Nocetti (2018).

by exploiting digital infrastructure to disrupt or destroy communication systems.

In his article ‘Cyber War Will Not Take Place’, Thomas Rid argues that such warfare, in the colloquial sense, has not yet occurred, instead manifesting itself through sabotage, intelligence activities and deception (Rid, 2012). By contrast, in their seminal article ‘Cyber War Is Coming’, published in *Comparative Strategy* in 1993, John Arquilla and David Ronfeldt describe it as a knowledge-based military conflict enabled by superiority in information and communication technologies and executed through knowledge, interception of communications and electronic obscuration (Arquilla & Ronfeldt, 1993).

Thus, we observe that this concept relies on four things:

- 1) the idea of military manoeuvring in virtual cyberspace;
- 2) executing this manoeuvre within or across cyberspace.
- 3) its role as an extension and complement to operations conducted in other regional dimensions; and 4) targeting pre-defined, diverse entities (states, individuals and proxies) through their electronic systems.

Therefore, we can conclude that cyber warfare acts as a force multiplier for military power, linked to operations conducted in other traditional domains.

Through the strategic activities adopted by various military bodies and institutions worldwide, we observe that cyberspace serves as a complement to operations in other domains aimed at controlling these territories. It appears to support all operations and manoeuvres undertaken by the state. A state’s strength in this field is measured by its technological capabilities and the human resources mobilised for this purpose. Thus, as noted by Daniel Foneur (Ventre, 2011), the concept of cyber warfare reinvigorates and activates the idea of power.

Conflict and rivalry between the US and Russia, for example, or between emerging states such as China, Russia, India and Brazil, in terms of traditional military capabilities or competitive fields such as economics, politics and culture, is also evident in cyberspace.

B. Cyber Espionage and the Concept of Cyber Power

Information and communication technologies are a factor of development for many states. There is a positive correlation between countries’ economic development and their connectivity to communication networks and access to cyberspace. The entry of emerging states into this space, in particular, has led to an increase in interstate conflicts among various international powers, as

evidenced by the significant growth in strategic cyber espionage activity.

Examining the concept of cyber power reveals the robust foundational relationship between espionage and power in this domain. Inspired by the notion of power in international relations, the concept of cyber power refers to a state's ability to exploit digital data to influence the behaviour of another actor in the international arena in order to achieve a specific goal (Noël, 2019).

Clearly, the concept of cyber power points explicitly to espionage activities and the capacity to utilise digital data for strategic purposes. However, it is important to note that the nature of power in this context differs from classical notions of power. Cyber power originates from the network itself, and its strength lies in what can be achieved within or across this space. An individual or company can become more powerful than a state, or even a coalition of states, by possessing the most formidable network in this space rather than through its resources. Here, 'stronger' refers to being 'smarter and more skilled' (Noël, 2019).

The sociological implication of this observation is that the human element is a key component of cyber power resources, which are embedded in the state's educational and formative systems. The 2018 edition of the Global Cybersecurity Index reflects this reality in the statement that 'the hard power of cyberspace is played out at university level' (Vanheste, 2020).

Since 2010, the United States, France, China and Russia have been considered to be among the strongest and most active countries in the field of cyber espionage. These countries' espionage systems rely on regional and global quasi-alliances. Current espionage systems primarily exploit traditional communication systems and the infrastructure provided by the physical layer of cyberspace, as mentioned above. These networks are supplemented by systems, software and programmes designed for this purpose (Diotte, 2020).

The Echelon system is the prime example of this model: a system for intercepting private and public communications, established by the US in alliance with Western European countries in 1947 and serving as infrastructure for other surveillance programmes. In 2013, Edward Snowden's leaks revealed the existence of the Prism programme, which spies on individuals, political figures, and European companies using the Echelon system's infrastructure.

C. Cyber warfare and cyber espionage as factors of cyber power

Given the contentious nature of cyberspace, as highlighted above, the goal of cyber warfare and cyber espionage is to control and dominate this space (Ventre, 2011). Traditionally, power was measured by the ability to control physical territories, but today it also encompasses the ability to regulate cyberspace. Therefore, control over this space is a strategic priority for all states seeking to protect their interests and security on the international stage.

Consequently, cyberspace has been reconfigured and its regional dimensions re-explored, as these dimensions have acquired strategic, operational and tactical significance through the extension of existing strategies, operations and tactics from other domains. We can therefore conclude that cyberspace gains its significance by linking it to conventional operations posed by the art of war in its broadest sense. Many prominent strategists and warfare experts today, for instance, embody and apply the principles of Chinese warfare set out by Sun Tzu in the 6th century BC regarding ‘surprise and stealth’, as well as Clausewitz’s notions about the ‘fog of war’ (Kempf, 2012).

Therefore, cyberspace is considered a factor that amplifies the power traditionally exercised in physical domains. However, controlling it requires the use of tools such as cyber warfare and cyber espionage, as well as other strategies. We will explore an example of this in the next section.

3. Towards Greater Control Over Cyberspace: An Analysis of the Concept of Digital Sovereignty Through the Example of Data Storage Centres’ Localisation’.

To illustrate how states respond to the challenges and issues posed by cyberspace by applying the principle of digital sovereignty through territorialisation of the physical layer, we will discuss a security measure adopted by some emerging states to reduce digital vulnerability and prevent data leaks to foreign spaces.

However, before that, we need to elaborate on the concept of digital sovereignty and mention some international experiences in this context.

3.1. The concept of digital sovereignty as a basis for cyber defence strategies

The concept of cyberspace seems to refer to a world rather than a territory with a physical presence. Nevertheless, our current reality is closely linked to the internet and devices connected to cyberspace, making it a domain with its own

authorities. Moreover, this domain was originally designed to resist authority and liberate itself from constraints imposed by states on their citizens and traditional territories.

If sovereignty, as defined by Jean Bodin in 1576, is “the absolute authority of the state over its territory, exercised in the name of its people”, how can a state control cyberspace or digital territory?

The initial responses to this question were negative, particularly among libertarians. The cyber libertarian movement supported the idea that the state only controls physical spaces within its territory, and cannot extend its authority to the digital realm. This viewpoint was prevalent at the dawn of the internet revolution and was bolstered by the novel argument that the internet could not be monitored or subjected to regulatory legislation (Johnson & Post, 1997).

However, in their 2006 book, Goldsmith and Wu refuted this argument, considering it an illusion and demonstrating that cyberspace can indeed be subjected to regulatory legislation. They argued that, as it is not centralised under a single authority, it consists of many entry points that can be used by the state to monitor and impose regulations on the methods and conditions of use (Goldsmith & Wu, 2006).

As previously noted, cyberspace is not merely amorphous; it has a material reality, represented by its physical layer and the individuals who create interconnections within and through this space. This makes the issue of regulation and subjection to state authority feasible. The growing body of regulations enacted by states regarding the modification and oversight of the digital space leaves no doubt that state policies are moving towards imposing legal sovereignty over this domain.

Conversely, additional dimensions of digital sovereignty are clarified through policies aimed at localising this space. This involves subjecting the physical layer of cyberspace to the direct authority of the state by establishing it within the state’s geographical territory.

3.2. Territorialising the Physical Layer: The Example of Data Storage Centres

Relocating data storage centres within territories directly under state control is a vivid example of policies based on digital sovereignty, which aim to address threats in cyberspace. The behaviour of emerging states in this area has been

influenced by the context created by Edward Snowden's revelations in 2013 about a comprehensive American surveillance programme targeting various countries, conducted by the NSA.

Russia, China, India and European Union countries have gradually matured in their approach, indicating that the era of absolute freedom in the flow of information through cyberspace has ended (Baur-Ahrens, 2017).

Presentation and analysis of the Russian case

In November 2017, Russian President Vladimir Putin approved a development plan to create an 'independent Russian internet' by 1 August 2018. In other words, the Russian government sought to establish Russia-specific domain names (DNS). These measures have continued to the present day, having been in place for around a decade, in order to promote Russian digital sovereignty. This sovereignty has become one of the key arguments underpinning Russian diplomacy in the field of cybersecurity governance, reflecting a desire to mitigate the effects of American hegemony (Epifanova, 2020).

Thus, the Russian strategy can be seen as an extension of its protests against American dominance in other areas. However, it is noteworthy that, in contrast to Western countries, which tend to favour transnational or supranational approaches, Russia has invested significant resources and efforts in the cybersecurity domain, adopting a sovereignty-based approach.

This tendency can be explained by a range of factors related to the geopolitical context at that time, particularly the repercussions of Edward Snowden's revelations about the extensive surveillance programmes of the US National Security Agency, which lent significant credibility to such decisions. It can also be attributed to the strong accusations made by the U.S. against Russia regarding interference in the 2016 presidential election, which created a diplomatic crisis of high tension between the two countries.

While these contextual explanations are relevant, there are also foundational interpretations that offer a more comprehensive explanation. The unique characteristics of Russian cyberspace render such decisions feasible, as well as politically and diplomatically ambitious. According to Kévin Limonier (2018), Russia is the only country in the world that possesses a comprehensive environment of platforms and digital services run by companies and individuals subject to Russian law.

While most of the world's population uses digital services offered by

American tech giants known as GAFAM (Google, Amazon, Facebook, Apple and Microsoft), Russians and speakers of Russian in other former Soviet states have the option to choose between American and Russian offerings across all digital domains. Evidence of this can be seen in the market share of search engines, which is divided between Google's American platform and Yandex, the Russian search engine. It is this unique environment that has enabled Russia to develop the technical, economic and political means to become a sovereign cyber power (Essam, 2021).

The Russian strategy for building a sovereign cyberspace is based on two main pillars: the economic and financial pillar, and the legislative pillar. Since 2015, the Russian government has invested substantially in developing digital infrastructure, particularly in localising data storage centres within Russia. In this context, large data storage centres have been constructed in the Siberian region to complement traditional installations distributed around major cities (Cattaruzza, 2020).

Legislatively, these substantial investments followed a law issued by the State Duma in July 2014 which came into force on 1 January 2016. This law requires all companies in the digital sector to store data relating to Russian citizens within Russian territory. This legislation demonstrates the Russian government's sovereign vision by applying the principle of territorial sovereignty to Russian cyberspace.

The plan reflects a strategic Russian outlook, particularly due to its regional, domestic and security benefits. Alongside the clear intention of re-establishing Russia's position in Central Asia, the plan aims to regenerate the Siberian region and mitigate desertification. Storing data within Russia represents a significant economic asset for digital sector companies managing data about individuals and institutions. From a security perspective, the Russian plan seeks to enhance the protection of Russian data and information, while limiting its leakage and migration into American cyberspace (Cattaruzza, 2020).

We have previously established that, as a domain of strategic activity, cyberspace fundamentally functions as a space of power. Therefore, it is important to recognise that adopting these protective policies based on the concepts of sovereignty and reterritorialisation cannot be justified solely by security considerations. Rather, they are policies and behaviours that reflect the extent of a state's strength and control over its territories.

Our examination of this new sovereign approach to managing cyberspace yields some important lessons and observations:

1) A change in the magnitude of the state's role and the extent of the authority it imposes on data, providers, and citizens.

2) Service-providing companies may alter their roles based on legal restrictions imposed by the state. They can transform from mere service providers into participants in the state's overall security apparatus by fulfilling protective requirements for users and consumers.

3) Users are positioned as a passive group, entirely subject to the scrutiny of both the state and providers.

Thus, we observe that policies aimed at localising cyberspace lead to changes in international power relations and are not purely security-based; they also seek to enhance the state's power and control in its traditional territories. The increasing number of states moving in this direction indicates a rising demand for such policies while simultaneously revealing an escalating international demand for renegotiation of the division of authority or power relations within this space. (Epifanova & Dietrich, 2022).

This renegotiation appears to extend beyond the technological nature of this space, pertaining also to prevailing power relations that are socially reproduced, as inspired by a Gramscian or Bourdieusian reading of cyber reality.

4. The challenges of digital transformation and the necessity of securing its cyberspace, according to a strategic vision

Cybersecurity in the digital era stands as the cornerstone for ensuring the continuity of electronic systems and safeguarding sensitive data, rendering it intrinsically linked to digital transformation across all sectors. Amid the accelerating pace of digital transformation, cybersecurity has evolved beyond a mere technical tool into a strategic imperative for ensuring its success. Any digital transformation must be fortified by a comprehensive cybersecurity network, underpinned by a robust digital infrastructure that safeguards data integrity, ensures information security, and upholds data confidentiality. (Mohamed, 2023, p. 12).

In the era of rapid digital transformation, institutions confront unprecedented security challenges stemming from expanded digital infrastructure, smart system integration, and the adoption of emerging technologies like cloud

computing, artificial intelligence, and the Internet of Things.

This swift evolution compels organizations to rethink cybersecurity strategies, making them more flexible, adaptive, and proactive. Digital transformation goes beyond mere system upgrades; it demands a comprehensive security ecosystem that matches the pace of change while protecting data, ensuring business continuity, and complying with regulatory standards.

4.1. Digital transformation is in an intertwined relationship with cyberspace:

Digital transformation improves operational efficiency and increases productivity; however, it simultaneously broadens the attack surface, creating more entry points that attackers can exploit to access systems. The emergence of technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT) has significantly reshaped the cybersecurity landscape.(Dessaints, n.d.)

These technologies also increase data vulnerability, as information is distributed across multiple systems and interconnected networks. With the growing reliance on digital services, it has become essential to develop advanced cybersecurity strategies capable of effectively addressing emerging and evolving threats.

There is a direct relationship between the level of digital transformation and the scale of cybersecurity requirements. As organizations adopt more advanced digital tools, new vulnerabilities emerge, increasing the need for stronger protection. These vulnerabilities often target devices and systems that are not adequately secured. (Ismail & Ben Kettaya, 2025).

At the same time, the rapid pace of digital transformation makes it difficult to keep up with evolving security challenges, which requires organizations to adopt flexible and adaptive cybersecurity strategies. Studies such as those conducted by Sasse and Bada (2019) show that organizations that fail to integrate cybersecurity from the early stages of digital transformation tend to experience significant gaps in their systems.

4.2. Cyberspace challenges in the context of rapid digital transformation:

Cybersecurity challenges are increasing alongside technological advancement and the rapid pace of digital transformation. This transformation can enhance the capabilities of cyberattacks, making them more sophisticated and complex. At the same time, the same technologies can be leveraged to strengthen

defense mechanisms and counter these threats, making digital transformation a double-edged sword. (schatz et al., 2017)

Among the positive aspects of digital transformation technologies in addressing advanced cyber threats is the role of data analytics in detecting unusual patterns and suspicious activities within cyber networks, which supports the early identification of potential attacks. In addition, automated response technologies can help mitigate the impact of cyberattacks by enabling systems to automatically isolate affected components, thereby limiting the spread of attacks and improving overall digital security.

With the intensification of cyber warfare driven by the contemporary digital revolution, the world is witnessing a new form of unconventional arms race. As cyberattacks increasingly escalate between states as well as between states and non-state actors, and as threats to national security continue to grow, there is an urgent need to develop a deeper understanding of cyberspace and the concept of cyber warfare. (Shams, 2025) It is also essential to examine the challenges these developments pose to national security, while exploring effective strategies and mechanisms to confront and mitigate their impacts.

The main challenge lies in achieving a delicate balance between preserving state sovereignty in cyberspace and safeguarding individuals' rights and freedoms. While some states seek to impose strict cyber regulations to protect their internal security and interests, such measures may negatively affect individuals' access to information and their freedom of expression. (Mahmoud, 2025) This raises a fundamental question about how to reconcile the requirements of cybersecurity with the protection of digital rights and civil liberties, ensuring that neither is prioritized at the expense of the other.

Accordingly, achieving cybersecurity stability requires the adoption of effective policies to address security vulnerabilities, confront risks, and mitigate the impacts of cybercrimes. States are increasingly preparing their capabilities to face future forms of warfare that rely on sabotage and destruction through cyberspace. In this context, cybersecurity has become a key component of the strategies of advanced countries, both for engaging in such conflicts and for countering them. Moreover, efforts to combat cyber threats have become an integral part of national defense strategies in many states (Aboud & Ibrahim, 2026).

5. Conclusion

Starting from the premise that cyberspace is a military space and a domain for strategic activity for states, similar to traditional state territories, we have attempted to understand its key characteristics and implications. This premise leads us to conclude that the same security challenges and threats exist in cyberspace.

Through our analysis of the geopolitical reality of this space, we have demonstrated that it reflects the existing power relations within the international community with regard to the hard structures of power in physical reality, and that it is a site of contention relating to states' aspirations to build or support power. Based on this observation, we concluded that the issues of contention in cyberspace merely reproduce the material and historical realities that frame international disputes.

Competition and conflict over power in the physical world engenders a new generation of competition and conflict in cyberspace. However, this universal characteristic is currently experiencing disruption and revision, reflecting new trends of the past decade — especially those relating to the implications of its use for states' sovereign issues. Cyberspace is shifting towards a 'Westphalian' model that organises spatial relations according to the concept of sovereignty.

The experiences of states with the intellectual resources to enhance their technological and knowledge-based capacities, such as Russia, China, India, Brazil, the European Union and Japan, highlight the growing global demand for cybersecurity policies based on digital sovereignty.

We have observed that cybersecurity policies and applications of the concept of digital sovereignty, as exemplified by Russia, provide greater security in Russian cyberspace while enhancing Russia's military and economic power in the cyber domain. This concept provides both researchers and policymakers with key strategic concepts through which other security and defence strategies can be constructed, offering both scientific and practical benefits.

In some countries, especially developing countries, the digital transition is struggling to achieve its objectives of creating economic wealth and opportunities for investment and business. Given the direct subordination and dominance imposed by major players in the digital field, both economically and technologically, it is challenging to speak of an economic experience.

Nevertheless, the digital transition has brought about a notable shift in e-governance and e-administration; however, this remains confined to specific sectors and is not part of a comprehensive public policy framework.

The pursuit of digital transformation requires the establishment of a high-level national authority dedicated to cybersecurity, along with the development of a comprehensive national strategy aimed at ensuring cybersecurity across various sectors and strengthening the state's readiness to address emerging digital challenges.

6. Footnotes and bibliography

- ¹ Aboud, W. F., & Ibrahim, M. (2026). Cybersecurity challenges. *Humanities & Natural Sciences Journal*, 7(2), 758–770. <https://doi.org/10.53796/hnsj72/47>
- ² Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is coming!* RAND Corporation. <https://www.rand.org/pubs/reprints/RP223.html>
- ³ Baur-Ahrens, A. (2017). The power of cyberspace centralisation: Analysing the example of data territorialisation. In *Security/Mobility*. Manchester University Press. <https://doi.org/10.7228/manchester/9781526107459.003.0003>
- ⁴ Cattaruzza, A. (2020). Cables, routes, and digital infrastructures: At the heart of international rivalries. <https://www.areion24.news/2020/07/07/cables-routes-et-infrastructures-numeriques-au-coeur-des-rivalites-internationales/>
- ⁵ Dessaints, A. (n.d.). How digital transformation impacts cybersecurity: Strategies, challenges, and best practices. DPO Consulting. <https://www.dpo-consulting.com/blog/digital-transformation-and-cybersecurity>
- ⁶ Diotte, P. (2020). The Big Four and cyber espionage: How China, Russia, Iran and North Korea spy online. *Canadian Military Journal*, 20(4), 32–42. <https://www.journal.forces.gc.ca/Vol20/No4/page32-eng.asp>
- ⁷ Epifanova, A. (2020, January 16). Deciphering Russia's "sovereign internet law": Tightening control and accelerating the splinternet. German Institute for International and Security Affairs (SWP). <https://www.swp-berlin.org/en/publication/deciphering-russias-sovereign-internet-law>
- ⁸ Epifanova, A., & Dietrich, P. (2022). Russia's quest for digital sovereignty: Ambitions, realities, and its place in the world. *DGAP Analysis*, 1, 1–27. <https://doi.org/10.60823/DGAP-22-36557>
- ⁹ Essam, A. (2021). Russia's use of cyber power in managing its international interactions. *Journal of the Faculty of Economics and Political Science*, 22(4), 167–190. <https://doi.org/10.21608/jpsa.2021.200069>
- ¹⁰ Gagnon, F., & Rapin, A. (2021). Cybersecurity in America: The US national security apparatus and cyber conflict management. In *Conflicts, Crimes and Regulations in Cyberspace* (pp. 43–62). John Wiley & Sons. <https://doi.org/10.1002/9781119885092.ch2>

11. Goldsmith, J., & Wu, T. (2006). Who controls the internet? Illusions of a borderless world. Oxford University Press. <https://doi.org/10.1093/oso/9780195152661.001.0001>
12. Ismail, M., & Ben Kettaya, H. (2025). Digital transformation and cybersecurity requirements: A literature review. University of Ghardaia.
13. Johnson, D. R., & Post, D. G. (1997). Law and borders: The rise of law in cyberspace. SSRN. <https://doi.org/10.2139/ssrn.535>
14. Kempf, O. (2012). Cyber strategy à la française. *Revue Internationale et Stratégique*, 87(3), 121–129.
15. Limonier, K. (2018). Sovereign cyberspaces? The case of Russia. Armand Colin. <https://www.cairn.info>
16. Mohamed, M. M. J. (2023). Digital transformation and the efficiency of legal and judicial systems: An analytical comparative study of 40 countries (1st ed.). Dar Al-Ahram for Publishing, Distribution and Legal Publications.
17. Mahmoud, K. W. (2025). Cyber borders and their impact on international relations: Challenges and strategic stability. *Rouya Türkiyyah*, 14(2), 199–218. <https://doi.org/10.36360/1560-014-002-010>
18. Nocetti, J. (2018). Geopolitics of cyber conflict. *Politique Étrangère*, Summer(2), 15. <https://doi.org/10.3917/pe.182.0015>
19. Noël, J.-C. (2019). What is digital power? (IFRI policy paper, Institut français des relations internationales, 2019, www.ifri.org/en/studies/what-digital-power).
20. Pegasus Project: Revelations about a global phone spying system. (2021, July 18). *Le Monde*. https://www.lemonde.fr/projet-pegasus/article/2021/07/18/projet-pegasus-revelations-sur-un-systeme-mondial-d-espionnage-de-telephones_6088652_6088648.html
21. Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32. <https://doi.org/10.1080/01402390.2011.608939>
22. Shams, N. (2025, June 27). Policies of digital transformation and cybersecurity. *Hura7*. <https://hura7.com/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A7%D8%AA->
23. Schatz, D., Bashroush, R., & Wall, J. (2017). Cybersecurity definition: A systematic analysis of cybersecurity definitions. *Journal of Digital Forensics, Security and Law*, 12(2).
24. Vanheste, A. (2020). What is a cyber power? <https://www.open-diplomacy.eu/blog/cyberpuissance-hackers-geopolitique-tech-gafa-batx>
25. Ventre, D. (2011). Cyberattack and cyber defence. Hermès Science Publications : Lavoisier.
26. Warusfel, B. (2021). La cyberdéfense, dimension numérique de la sécurité nationale. In S.-Y. Laurent (Ed.), *Conflits, crimes et régulations dans le cyberspace*. ISTE Éditions