International Journal Of History And Political Sciences

VOLUME Vol.06 Issue05 2026
PAGE NO. 39-47
DOI 10.37547/ijhps/Volume06Issue05-07

Cyber Geopolitics and Digital Transformation: Contemporary Challenges to Regional Security

Saodat Ubaydullaeva
Tashkent State University of Oriental Studies Tashkent, Uzbekistan

Received: 29 March 2026; **Accepted:** 25 April 2026; **Published:** 20 May 2026

Abstract: Digital transformation has changed many areas of modern society, including economics, politics, communication, and security systems. Governments, regional organizations, and private institutions increasingly depend on digital technologies for administration, infrastructure, financial systems, and information exchange. At the same time, cyber threats have become more complex and more difficult to control. Cyberattacks, digital espionage, information manipulation, and attacks on critical infrastructure are now affecting regional stability in different parts of the world. This article examines the relationship between cyber geopolitics and digital transformation and how this process creates new challenges for regional security. The study focuses on the growing role of cyberspace in geopolitical competition between states and the security risks connected with rapid digitalization. The research also discusses cyber warfare, hybrid threats, digital sovereignty, and the influence of artificial intelligence in cybersecurity strategies. The article uses qualitative and comparative analysis based on academic literature, international cybersecurity reports, and recent regional examples. Different regions and global actors are compared to understand how digital transformation changes modern security policies and geopolitical relations.

The findings show that digital transformation creates both opportunities and vulnerabilities. While digital systems improve communication, economic growth, and state management, they also increase exposure to cyber risks and political pressure in cyberspace. The study shows that regional cooperation, stronger cybersecurity policies, and international digital governance are becoming necessary for maintaining regional stability in the digital era.

Keywords: Political Competence, Social Protection, National Agency for Social Protection, Digital Meritocracy, Digital Political Immunity, Executive Leadership, Social State, Uzbekistan-2030, Public Administration Modernization, Political Empathy.

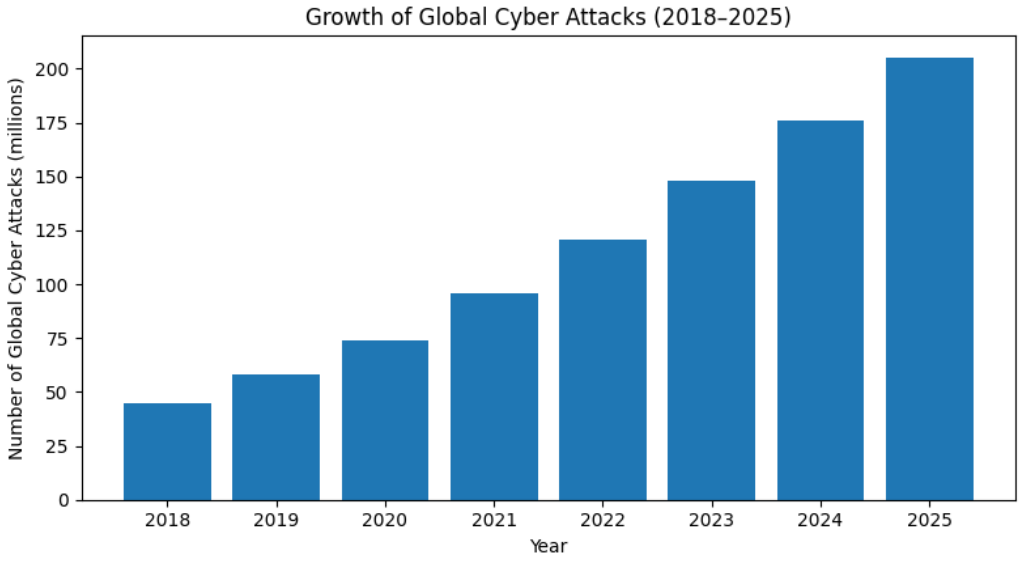
Introduction: Digital transformation has accelerated rapidly during the last decade. Governments, businesses, educational institutions, and healthcare systems increasingly rely on digital technologies for communication, administration, financial operations, and data management. Technologies such as artificial intelligence, cloud computing, big data, blockchain, and smart infrastructure continue to reshape both economic and political systems. This process has improved efficiency and connectivity, but it has also created new security vulnerabilities in cyberspace.

Many states now depend heavily on digital systems and online infrastructure. Public administration, military communication, transportation systems, energy networks, and banking services are connected through digital platforms. Because of this dependence, cyberattacks may affect not only technical systems but also national stability and regional security. Cyber incidents targeting critical infrastructure have become more frequent in recent years, creating economic losses and political tensions between countries. The increase in cyber threats has changed the traditional understanding of security. In the past, security discussions mainly focused on military conflict, territorial disputes, and economic competition. Today, cyberspace has become another important area of geopolitical rivalry. States compete for technological superiority, digital influence, and control over strategic information systems. Cyber capabilities are increasingly viewed as part of national power.

Cyber threats now include cyber espionage, ransomware attacks, disinformation campaigns, digital surveillance, attacks on critical infrastructure, and hybrid warfare operations. Some attacks are conducted by organized criminal groups, while others are linked to political or geopolitical interests. Information manipulation through social media platforms has also become a major concern because false information may influence elections, increase social tensions, and weaken trust in public institutions. The rapid spread of digital technologies has also increased competition between global powers. Countries such as the United States, China, and Russia continue investing heavily in cyber capabilities, artificial intelligence, and digital infrastructure. Technological competition is now closely connected with geopolitical strategy. Control over digital technologies, data systems, and communication networks may provide political and economic influence at both regional and global levels.

The following figure was selected to show the visible increase in cyberattacks during the period of rapid global digitalization. The data helps explain why cybersecurity has become one of the central issues in regional and international security discussions. The figure below presents the rapid increase in global cyberattacks between 2018 and 2025. The chart was included to demonstrate how accelerated digital transformation and increasing dependence on online infrastructure have expanded cybersecurity risks worldwide Fig 1.

Figure 1. Growth of Global Cyber Attacks (2018–2025)



Bar Chart: Global Cyber Attacks (2018–2025)

The data shows a steady rise in cyberattacks over the examined period. In 2018, global cyber incidents were estimated at 45 million, while by 2025 the number reached 205 million. The sharp increase after 2020 reflects the growing use of cloud technologies, remote work systems, digital financial services, and online communication platforms. The figure also indicates that cybersecurity threats are increasing together with global digitalization. As governments and organizations become more dependent on digital systems, critical infrastructure becomes more vulnerable to cyberattacks, ransomware operations, and information security breaches.

The article is important because digital transformation continues expanding faster than many national cybersecurity systems can adapt. Understanding the geopolitical dimension of cyberspace may help states and regional organizations improve digital security policies and respond more effectively to emerging cyber threats.

Literature Review

The concept of cyber geopolitics emerged together with the rapid expansion of digital technologies and global internet infrastructure. Traditional geopolitics mainly focused on territorial control, military power, and economic influence. Today, cyberspace has become another important strategic environment where states compete for influence, information control, and technological superiority. Digital infrastructure, cyber capabilities, and information systems are now closely connected with political and security interests (Liebetrau & Monsees, 2024).

Cyberspace is increasingly viewed as a strategic domain similar to land, sea, air, and outer space. Governments invest heavily in cybersecurity systems, cyber intelligence, artificial intelligence, and digital surveillance technologies. Strong cyber capabilities

may provide economic, military, and political advantages in international relations. Because of this, cyber power has become part of national power (Khan, 2025).

Many researchers explain cyber geopolitics through different theoretical perspectives. Realist approaches focus on state competition and national interests in cyberspace. Liberal perspectives support international cooperation and collective cybersecurity mechanisms. Constructivist theories pay more attention to information influence, social perception, and digital narratives in shaping political behavior and security threats (Glasze et al., 2022).

The rapid development of digital technologies has also increased discussions about digital sovereignty and technological dependence. States increasingly attempt to strengthen control over national digital infrastructure, strategic technologies, and data systems in order to reduce geopolitical vulnerability and external influence (Falkner et al., 2024).

The following table was included to compare the main theoretical approaches used in cyber geopolitical studies and to explain how different theories interpret cybersecurity and digital conflicts Table 1.

Table 1. Major Approaches in Cyber Geopolitical Theory

Theory	Main Idea	Security Perspective
Realism	States compete for power and strategic advantage in cyberspace	Cyber capability strengthens national security and state influence
Liberalism	International cooperation may reduce cyber risks and instability	Shared cybersecurity frameworks improve regional stability
Constructivism	Political narratives and information shape cyber conflicts	Digital information influences social and political security
Technological Determinism	Technology changes political structures and security systems	Digital transformation reshapes modern conflict patterns

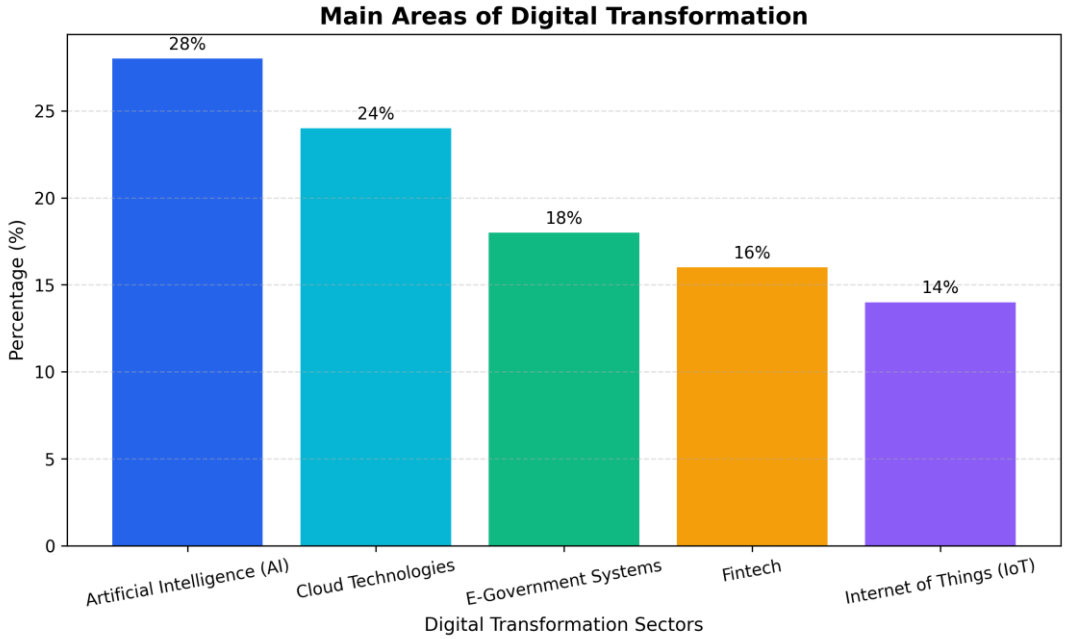
Table 1 shows that realist perspectives remain highly influential in current cyber conflicts because many states increasingly prioritize cyber power, strategic technologies, and digital sovereignty. However, liberal approaches also remain important due to the growing need for international cybersecurity cooperation and information sharing. Constructivist theories are especially relevant in understanding information warfare, online propaganda, and digital influence campaigns.

The literature also shows that cyberspace differs from traditional geopolitical environments because cyber operations are often difficult to trace. Attribution problems make it challenging to identify the real actor behind cyberattacks. This uncertainty increases political tension and complicates international responses to cyber incidents (Steingartner & Galinec, 2021). Another issue discussed in many studies is the militarization of cyberspace. Some governments now integrate cyber operations into military strategy and national defense planning. Cyber warfare capabilities are increasingly viewed as strategic assets that may influence regional power balance and geopolitical competition (Khan, 2025).

Digital transformation has significantly changed the way states manage administration, communication, security, and economic systems. Governments increasingly adopt digital technologies to improve efficiency, public services, and information management. E-government systems, artificial intelligence, cloud technologies, smart infrastructure, and big data platforms are now widely used in both developed and developing countries (Saeed et al., 2023). Digital technologies create many advantages for state administration. E-government systems improve communication between governments and citizens, reduce bureaucracy, and simplify public services. Smart infrastructure helps manage transportation, healthcare, energy systems, and urban planning more effectively. Artificial intelligence supports data analysis, cybersecurity monitoring, and automated decision-making processes (Abisoye & Akerele, 2022). At the same time, digital transformation also creates new security vulnerabilities. As states become more dependent on interconnected systems, cyber risks increase. Weak digital protection systems may expose sensitive information, financial systems, and critical infrastructure to cyberattacks and espionage activities (Serac, 2023).

The following chart presents the main areas of digital transformation that currently influence state development and cybersecurity policy Fig 2.

Figure 2. Main Areas of Digital Transformation



The figure demonstrates that artificial intelligence and cloud technologies currently represent the fastest-growing sectors of digital transformation. AI systems are increasingly used in cybersecurity, financial systems, surveillance technologies, and public administration. Cloud technologies continue expanding because governments and businesses require large-scale digital storage and online infrastructure.

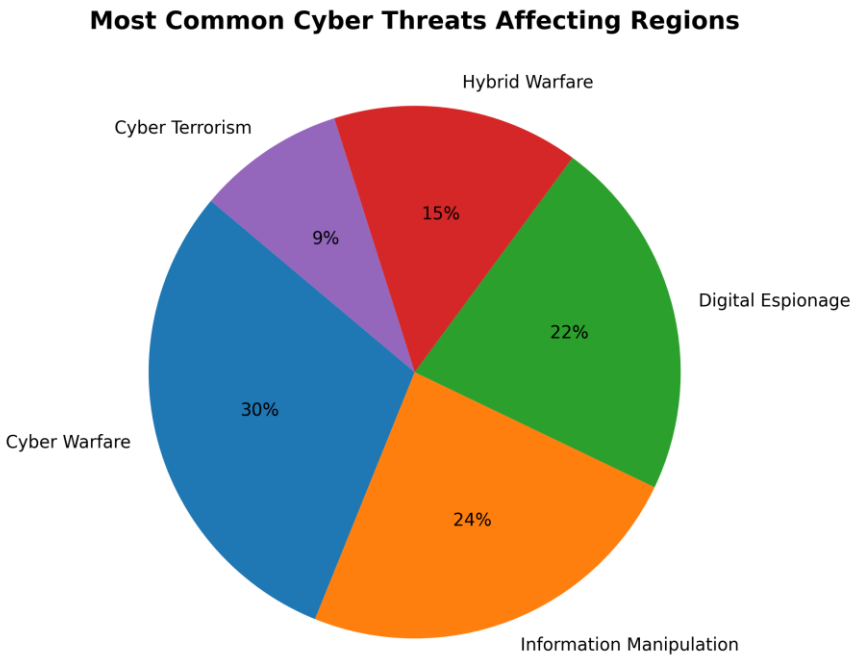
The literature also shows that IoT systems and smart infrastructure create both convenience and vulnerability. Connected devices improve communication and automation, but they may also become targets for cyber intrusions if cybersecurity protection remains weak.

Another important issue is the growing dependence on foreign digital technologies and software systems. Many states rely on external cloud services, communication platforms, and digital infrastructure controlled by foreign companies. This dependence may increase geopolitical risks and reduce digital sovereignty during periods of international tension.

Cyber threats have become one of the main challenges affecting regional security in the digital era. The development of digital infrastructure and online communication systems has expanded opportunities for cybercrime, cyber warfare, and information manipulation. Modern cyber threats often affect not only individual organizations but also entire regions and national security systems. Cyber warfare is increasingly connected with geopolitical competition. Some cyberattacks target critical infrastructure such as transportation systems, banking networks, energy facilities, and government databases. These attacks may disrupt public services and create political instability. Cyber warfare is often used together with political pressure, economic sanctions, and information campaigns. Hybrid warfare has also become an important concern in regional conflicts. Hybrid threats combine cyberattacks, misinformation, propaganda, political influence operations, and economic pressure. Social media platforms are frequently used to spread false information and manipulate public opinion during political crises or elections. Digital espionage represents another major cybersecurity challenge. Governments, corporations, and political organizations are often targeted by cyber actors attempting to steal confidential information, technological data, or strategic intelligence. Cyber espionage activities may continue for long periods without detection.

The following chart presents some of the most common cyber threats affecting regional security Fig 3.

Figure 3. Most Common Cyber Threats Affecting Regions



(Bar chart will be inserted based on the outher.)

The chart indicates that cyber warfare and information manipulation are among the most significant cyber threats affecting regions today. Cyberattacks targeting government institutions and critical infrastructure continue increasing in many parts of the world. Information manipulation through digital platforms has also become a serious political and social problem because it may influence elections, increase polarization, and weaken public trust. The literature suggests that regional organizations and governments must improve cybersecurity coordination, intelligence sharing, and digital protection systems to reduce these risks effectively. Digital sovereignty has become an important issue in modern international relations. Governments increasingly attempt to strengthen control over national data, communication infrastructure, and digital technologies. Many states view technological independence as part of national security and geopolitical strategy.

Competition between the United States and China represents one of the central aspects of global cyber geopolitics. Both countries invest heavily in artificial intelligence, semiconductor technologies, cloud infrastructure, and cybersecurity systems. Technological competition between these powers increasingly affects global trade, digital governance, and international political relations. Russia also plays a significant role in cyber geopolitics, especially through information warfare strategies and cyber influence operations. Russian cyber activities are often discussed in relation to disinformation campaigns, cyber espionage, and political influence operations targeting foreign states.

NATO has expanded its cybersecurity policies in response to growing cyber threats and hybrid warfare risks. Cyber defense is now considered part of collective security strategy. Many NATO members continue increasing investment in cybersecurity infrastructure, cyber defense units, and digital resilience programs.

The following table compares the cyber strategies of major global powers and their primary objectives in cyberspace.

Table 2. Cyber Strategies of Major Global Powers

Country	Cyber Strategy	Main Objective
United States	Advanced cybersecurity systems and AI investment	Maintain global technological leadership
China	Digital expansion and technological self-sufficiency	Increase digital sovereignty and global influence
Russia	Information warfare and cyber influence	Strengthen geopolitical influence

Country	Cyber Strategy	Main Objective
	operations	
European Union	Data protection and regional cooperation	cybersecurity Improve digital security and regulatory control
NATO	Collective cyber defense strategy	Protect member states from cyber threats

Table 2 demonstrates that major powers approach cybersecurity from different strategic perspectives. The United States and China focus heavily on technological leadership, while Russia emphasizes information influence and geopolitical strategy. The European Union and NATO prioritize digital regulation, collective security, and regional cybersecurity cooperation.

The literature also shows that technological dependence remains a major concern for many developing countries. States that rely heavily on foreign digital infrastructure may face political and economic vulnerability during geopolitical crises. Because of this, digital sovereignty is increasingly connected with national security, economic stability, and regional geopolitical competition.

Methods

This study uses a qualitative research approach to examine the relationship between cyber geopolitics, digital transformation, and regional security. A qualitative method was selected because the topic mainly focuses on political processes, cybersecurity challenges, technological developments, and geopolitical competition in cyberspace (Liebetrau & Monsees, 2024). The research is based on comparative and analytical methods. Different regional and international cybersecurity situations were compared to understand similarities and differences in cyber threats, digital policies, and geopolitical strategies. Attention was given to how states respond to cybersecurity challenges and how technological development changes regional security environments (Ferrag et al., 2023).

Data for the study was collected from academic journals, cybersecurity reports, government publications, international organization reports, and digital security studies published in recent years. Sources from international institutions such as NATO, the European Union, the United Nations, the World Economic Forum, and global cybersecurity organizations were also examined to understand current cyber trends and regional security issues (Saeed et al., 2023). The study mainly relies on secondary data analysis. Existing academic literature and international cybersecurity statistics were reviewed to identify major patterns related to cyber warfare, hybrid threats, digital sovereignty, and cyber competition between global powers. Reports discussing cyberattacks, digital infrastructure vulnerability, and information warfare were particularly important in the analytical process (Steingartner & Galinec, 2021).

Content analysis was used to examine political strategies, cybersecurity policies, and digital transformation programs implemented by different states and regional organizations. This method helped identify the main security concerns connected with rapid digitalization and geopolitical rivalry in cyberspace (Falkner et al., 2024). Comparative analysis was also used to evaluate differences between developed and developing regions in terms of cybersecurity preparedness, technological dependence, and digital resilience. The comparison helped explain why some regions are more vulnerable to cyber threats and digital instability (Abisoye & Akerele, 2022).

The research does not focus on one individual country only. Instead, it examines broader regional and international trends connected with cyber geopolitics and digital transformation. Examples from the United States, China, Russia, the European Union, and other regions were included to provide a wider understanding of modern cybersecurity challenges (Glasze et al., 2022). One limitation of the study is that cyber threats and digital technologies change very rapidly. New cyber incidents, technological innovations, and geopolitical developments continue emerging, which may affect future cybersecurity conditions differently from current observations. Another limitation is the difficulty of obtaining complete information about some cyber operations because many states treat cybersecurity activities as confidential or strategically sensitive information (Serac, 2023). Despite these limitations, the study provides a broader understanding of how digital transformation and cyber geopolitics influence regional security in the modern digital era (Khan, 2025).

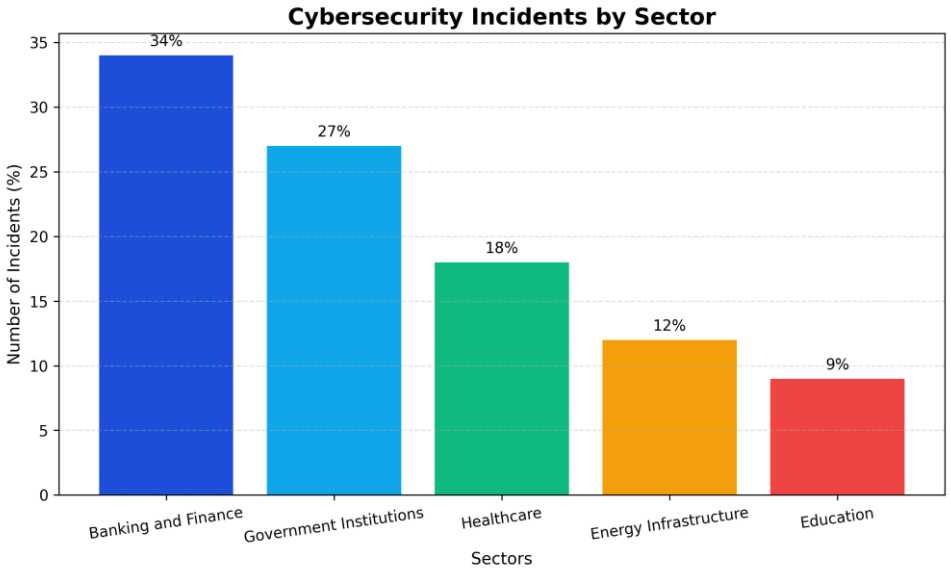
Results and Discussion

The findings show that rapid digital transformation has significantly increased cybersecurity risks in many regions of the world. Governments, financial institutions, healthcare systems, and communication networks have become more dependent on digital

infrastructure during the last decade. This dependence improved efficiency and connectivity, but it also expanded the number of possible cyber vulnerabilities (Saeed et al., 2023). One of the main problems identified in the analysis is the weak cybersecurity protection of critical infrastructure. Many organizations continue adopting cloud systems, artificial intelligence, and online platforms faster than they improve cybersecurity systems. As a result, cybercriminal groups and politically motivated actors gain more opportunities to target sensitive information and public infrastructure (Schmitt, 2023). Recent cyber incidents demonstrate how digital dependence may affect regional stability. Ransomware attacks against hospitals, energy companies, transportation systems, and banking networks have disrupted public services in several countries. Some attacks caused financial losses, temporary infrastructure shutdowns, and information leaks involving millions of users (Wells, 2022). The analysis also shows that developing regions often face greater cybersecurity challenges because of weaker digital protection systems and limited technological resources. Shortages of cybersecurity specialists and outdated infrastructure increase vulnerability to cyberattacks and digital espionage activities (Serac, 2023).

The following statistics present some of the sectors most frequently affected by cybersecurity incidents during rapid digital transformation.

Figure4. Cybersecurity Incidents by Sector



The figure shows that banking and financial systems remain the most targeted sectors because they store large amounts of financial and personal data. Government institutions are also major targets due to political motivations, intelligence collection, and cyber espionage activities. Healthcare systems experienced growing cyber risks after digital medical records and online healthcare services became more common.

Another important result of the study is the increasing use of artificial intelligence in cyber operations. AI technologies are now used not only for cybersecurity protection but also for cyberattacks, phishing operations, automated hacking attempts, and deepfake content creation. This development complicates cybersecurity defense systems because cyber threats become faster and more adaptive. The analysis demonstrates that cyber threats affect regions differently depending on technological development, political conditions, and cybersecurity preparedness. Developed countries generally have stronger cybersecurity systems and better digital infrastructure, while developing regions often face greater technological vulnerability. In Europe, cybersecurity policies are strongly connected with data protection, digital regulation, and regional cooperation. The European Union continues investing in digital resilience and cybersecurity coordination among member states. However, European countries still experience cyber espionage activities, ransomware attacks, and information manipulation campaigns targeting political systems and public institutions. Central Asian countries are rapidly expanding digital infrastructure and e-government systems, but cybersecurity protection mechanisms remain uneven across the region. Some states continue depending heavily on foreign technologies and external digital platforms. Limited cybersecurity investment and shortages of trained specialists create additional regional vulnerabilities. The Asia-Pacific region has become one of the main centers of technological competition and cyber geopolitical rivalry. The increasing influence of China, growing digital infrastructure projects, and regional

security tensions contribute to rising cyber risks. Many countries in the region continue strengthening cybersecurity systems because of concerns related to cyber espionage and information security. The Middle East also faces serious cybersecurity challenges due to political instability, regional conflicts, and attacks targeting energy infrastructure. Oil and gas systems remain highly important targets because disruptions in these sectors may affect both regional economies and global energy markets.

The following table summarizes some of the major cybersecurity challenges affecting different regions.

Table 3. Regional Cybersecurity Challenges

Region	Main Threat	Security Impact
Europe	Information manipulation and ransomware	Political instability and data breaches
Central Asia	Weak cybersecurity infrastructure	Increased digital vulnerability
Asia-Pacific	Cyber espionage and technological rivalry	Regional geopolitical tension
Middle East	Attacks on energy infrastructure	Economic and security disruption

The table demonstrates that cybersecurity threats are closely connected with regional political and economic conditions. Different regions prioritize different cybersecurity strategies depending on their technological capacity and geopolitical environment. The study shows that cyberspace has become an important area of geopolitical competition between global powers. States increasingly compete through technological development, digital infrastructure control, cybersecurity systems, and artificial intelligence capabilities.

The United States and China currently dominate many areas of global digital competition. Both countries invest heavily in artificial intelligence, cloud infrastructure, semiconductor production, and cybersecurity research. Their competition affects global technological supply chains, digital trade, and international political relations (Falkner et al., 2024). Russia continues using cyber influence operations and information warfare strategies as part of its geopolitical approach. Cyber activities connected with disinformation campaigns and digital influence operations remain important concerns in international cybersecurity discussions (Steingartner & Galinec, 2021). The findings also show that technological dependence creates security risks for smaller and developing states. Countries relying heavily on foreign digital platforms, cloud systems, or communication technologies may become vulnerable to political pressure and cyber influence during periods of international tension (Glasze et al., 2022).

Another important issue identified in the study is the fragmentation of international cybersecurity governance. Many countries support cybersecurity cooperation in theory, but practical cooperation often remains limited because states prioritize national interests and strategic competition (Liebetrau & Monsees, 2024).

Conclusion

Digital transformation has become one of the main forces shaping modern political, economic, and security systems. The rapid expansion of artificial intelligence, cloud technologies, digital infrastructure, and online communication platforms has changed how states operate and interact with each other. At the same time, the growing dependence on cyberspace has created new security risks that increasingly affect regional stability and international relations. The study showed that cyber geopolitics is now an important part of global power competition. States no longer compete only through military strength or economic influence. Technological superiority, cybersecurity capacity, digital infrastructure, and control over information systems have become major strategic factors in modern geopolitics. Cyberspace has developed into a strategic domain where political influence, cyber espionage, and information warfare continue expanding. The analysis also demonstrated that cyber threats are becoming more complex and more interconnected with regional security challenges. Cyber warfare, hybrid threats, digital espionage, ransomware attacks, and information manipulation increasingly affect governments, financial systems, healthcare institutions, and critical infrastructure. In many cases, cyber incidents create not only technical problems but also political tension, economic disruption, and public instability. Another important finding is the unequal level of cybersecurity preparedness between regions. Developed countries generally possess stronger digital infrastructure and cybersecurity systems, while many developing regions continue facing technological dependence, weak cyber protection, and shortages of qualified specialists. This situation increases vulnerability to cyberattacks and geopolitical pressure in cyberspace.

The study also highlighted the growing importance of

digital sovereignty in international relations. Many states are attempting to strengthen control over national data, communication technologies, and digital infrastructure in order to reduce external dependence and improve national security. Competition between major powers such as the United States, China, and Russia continues influencing global cybersecurity policies and technological development.The findings suggest that stronger cybersecurity strategies and international cooperation will become increasingly necessary in the future. Cyber threats often cross national borders and involve multiple actors operating in different regions. Because of this, regional organizations and governments need to improve information sharing, cybersecurity coordination, and digital resilience. Future security environments will likely depend heavily on technological innovation, artificial intelligence development, and the ability of states to protect critical digital infrastructure. As digital transformation continues expanding, cybersecurity will remain one of the central issues affecting regional stability and geopolitical relations in the modern world.

References

1. Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors (Basel, Switzerland), 23. https://doi.org/10.3390/s23156666.
2. Serac, C. (2023). DIGITAL TRANSFORMATION VULNERABILITIES: ASSESSING THE RISKS AND STRENGTHENING CYBER SECURITY. THE ANNALS OF THE UNIVERSITY OF ORADEA. ECONOMIC SCIENCES. https://doi.org/10.47535/1991auoes32(1)059.
3. Khan, Z. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. The Critical Review of Social Sciences Studies. https://doi.org/10.59075/k9cbhz04.
4. Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security. https://doi.org/10.34190/eccws.22.1.1443.
5. Steingartner, W., & Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. https://doi.org/10.12700/aph.18.3.2021.3.2.
6. Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. Geopolitics, 28, 919 - 958. https://doi.org/10.1080/14650045.2022.2050070.
7. Mustata, A., & Potcovaru, S. (2025). From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats. BULLETIN OF "CAROL I" NATIONAL DEFENCE UNIVERSITY. https://doi.org/10.53477/2284-9378-25-51.
8. Wells, J. (2022). Preparing for hybrid warfare and cyber-attacks on health services' digital infrastructure: what nurse managers need to know.. Journal of nursing management. https://doi.org/10.1111/jonm.13633.
9. Abisoye, A., & Akerele, J. (2022). A Practical Framework for Advancing Cybersecurity, Artificial Intelligence and Technological Ecosystems to Support Regional Economic Development and Innovation. International Journal of Multidisciplinary Research and Growth Evaluation. https://doi.org/10.54660/.ijmrge.2022.3.1.700-713.
10. Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. Journal of European Public Policy, 31, 2099 - 2120. https://doi.org/10.1080/13501763.2024.2358984.
11. Adonis, A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. Global: Jurnal Politik Internasional. https://doi.org/10.7454/global.v21i2.412.
12. Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. J. Ind. Inf. Integr., 36, 100520. https://doi.org/10.1016/j.jii.2023.100520.
13. Ferrag, M., Kantzavelou, I., Maglaras, L., & Janicke, H. (2023). Hybrid Threats, Cyberterrorism and Cyberwarfare. https://doi.org/10.1201/9781003314721.
14. Kaur, R., Gabrijelcic, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Inf. Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804.
15. Liebetrau, T., & Monsees, L. (2024). Cybersecurity and International Relations: developing thinking tools for digital world politics. International Affairs. https://doi.org/10.1093/ia/iiae232.