

Scientific and Digital Advancement, Major Powers' Mastery of Artificial Intelligence Technology, and Its Impact on Cybersecurity Control in Third World Countries

Dr. Moulay Boumedjout

Faculty of Law and Political Science, University of Blida 2 - Ali Lounici

Email: boumedjout.moulay@gmail.com

Received: 10/02/2026 ; Accepted: 03/08/2026 ; Published: 13/09/2026

Abstract

At the beginning of the new millennium, the world witnessed a major wave of scientific and technological advancement. New variables emerged. After digitization and the digital transformation that accompanied the spread of the Internet, a new, faster, more precise, and more comprehensive development appeared: artificial intelligence. AI has become a powerful instrument in the hands of states that master its scientific foundations and practical applications. According to many experts, this mastery enables such states to exercise control over international cybersecurity. This has intensified competition among major powers for mastery of artificial intelligence technology. Amid this rivalry, Third World countries remain significantly behind in digitalization and AI-related technological and knowledge capabilities. They rely largely on imported Western or Chinese software systems over which they have limited control. This dependence has significantly affected their cybersecurity and, consequently, their overall security systems.

Keywords: Artificial Intelligence (AI) ; Cybersecurity ; Digital Transformation ; Technological Dependence ; Third World Countries Introduction

After the end of the Cold War, the international arena underwent structural and profound changes in the composition of the international system. The world moved toward unipolarity and Western-centered decision-making under the leadership of the United States. The United States did not adopt a policy of strategic passivity. Instead, it moved rapidly to accumulate further power, subject the world to its control and hegemony, prevent the emergence of future rival poles, and expand its influence over Third World countries. The third and fourth scientific and technological revolutions strengthened its power, reinforced its dominance over global decision-making, and increased its capacity to Americanize international relations. Western comprehensive power was no longer confined to geographical factors or conventional military capabilities. It increasingly rested on technological control and command of advanced digital knowledge. This technological wave also created a complex network of interconnected relations and mutual dependence among international actors, including both advanced states and countries that lagged behind technological development. Yet this interdependence contains a structural and unequal imbalance between advanced states, especially the Western bloc led by the United States, and Third World countries, most of which belong to the Global South.

At the beginning of the third millennium, the world moved beyond the conventional digital environment and the traditional Internet toward the age of artificial intelligence. AI has become one

of the most sensitive and consequential variables in the international power equation. It is no longer merely a tool for facilitating services or promoting economic development. It has become a strategic instrument that can provide states possessing its technologies with extensive capacity to influence and control the international cyber domain.

While major powers, led by the United States and China, compete to control algorithms and large-scale data repositories, Third World countries remain primarily consumers and importers of these technologies. This position leaves their national and cyber security highly exposed. The resulting dependence also affects their financial, military, normative, and societal sectors.

Against this background, this study examines the dimensions and risks of technological and artificial intelligence control by major powers and assesses its implications for cybersecurity in Third World countries.

Main Research Question:

- **How do scientific and digital superiority and major powers' control of artificial intelligence technology reinforce cyber hegemony and deepen the comprehensive dependence of Third World countries?**

Core Hypotheses:

1. The unilateral or bilateral possession of artificial intelligence technologies and international digital networks by major powers turns cyberspace into an instrument of economic and military hegemony.
2. Technological dependence and the direct use of Western and Chinese software contribute to breaches of the cybersecurity systems of Third World countries and to the exposure of their sovereign national data.

Section One: Digital Advancement and Its Role in Reshaping the Rules of Power and International Hegemony

Recent years have witnessed an exceptional acceleration in technological development. Discussion has moved beyond digital dominance toward a broader and more comprehensive technological sphere. Researchers increasingly regard this shift as one of the most advanced scientific transformations, with the potential to alter the balance of power and redefine the variables that shape global power relations. This section therefore identifies the main components of digital power, provides a conceptual account of the notion, and examines its influence on changes in the global balance of power.

First: The Digital Transition after the Cold War

The end of the Cold War was a strategic turning point in the history of international relations. It led to the collapse of bipolarity and the emergence of a unipolar international system led by the United States. The United States used its scientific and digital superiority to consolidate control over the infrastructure and tools of international communication. The transition of the international community from an industrial society to a knowledge- and digital-based society increased interdependence among states. At the same time, it widened the technological gap between the developed world and developing countries. British scholar Rowley defines digital development as "the set of scientific, technological, engineering, and administrative systems used to handle and

process information and its applications, as well as their interaction with people and devices, together with the related social, economic, and cultural dimensions."¹

Developed countries have consequently acquired the mechanisms needed to control knowledge resources, software production, and technological capabilities. Third World countries, by contrast, have remained unable to localize these technologies. This has created a form of structural inequality within the international system and its patterns of interaction.²

Second: Control of Financial and Economic Institutions and Systems through Digital Infrastructure (SWIFT as a Model)

Western interest, especially that of the United States, in international financial and monetary institutions dates back to the Bretton Woods Agreement of 1944. The agreement laid out an integrated project aimed at securing future control over key components of the global economy. This encouraged the development of a scientific base capable of supporting technological superiority and an international financial system subject to direct monitoring and guidance. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is presented as one of the clearest manifestations of this form of digital financial dominance.

The acronym "SWIFT" stands for "Society for Worldwide Interbank Financial Telecommunications."

The system was established in 1973, and the organization is headquartered in La Hulpe, Belgium, near Brussels. SWIFT connects approximately 11,000 banks and institutions in more than 200 countries. According to the national association known as "Rosswift," Russia is the second-largest country within SWIFT in terms of the number of users after the United States, with around 300 financial institutions. According to the association, these members account for more than half of the financial institutions in the country.³

SWIFT connects central and commercial banks around the world through a complex physical and software infrastructure located in Western countries and controlled by the United States. This position enabled U.S. authorities to impose precise and continuous monitoring mechanisms over international financial flows. Technological control also became an instrument for imposing severe and effective economic sanctions on any state classified as rogue or opposed to U.S. policies. Foremost among these cases are Iran, Iraq under the late President Saddam Hussein, and Syria following the Caesar Act sanctions approved by President Trump against the Assad regime. Excluding a bank or a state from this system can cause near-total economic and commercial paralysis, as occurred in practice.⁴

The foregoing makes clear that the United States, together with other Western countries, sought to establish global financial and economic dominance. This project was planned even before the creation of the major international political institutions. The Bretton Woods Agreement formed a

¹ Rowley, J. E., *The Basics of Information Technology*, Clive Bingley, London, 1988, p. 63.

² Abdelkader Mohamed, *International Relations in the Digital Age: From Geopolitics to Geo-Cyber Politics*, Dar Al-Nahda Al-Arabiya, Cairo, 2018, p. 45.

³ Russell Hotten, "What Is the SWIFT Global System, and Why Is the West Divided over Excluding Russia from It as Punishment?" BBC Arabic, 25 February 2022, accessed 31 August 2026, <https://www.bbc.com/arabic/world-60524465>

⁴ Ibrahim Al-Ali, "The International Monetary System and the Weapon of Digital Sanctions," *International Politics*, No. 210, Al-Ahram Center for Political and Strategic Studies, Cairo, Egypt, 2020, p. 88.

basic foundation for future Western control over key components of the global economy, led by the United States. Technological and digital development further consolidated this Western project and enabled the West to exercise extensive control over the global economic landscape and international banking and monetary systems. The West, and the United States in particular, did not limit itself to controlling international financial institutions and using them as effective instruments to pressure states and alter their political and economic approaches, as occurred with socialist countries during the 1980s. It also moved toward linking central banks around the world to the U.S.-centered financial system through SWIFT. In addition, the U.S. dollar became a global currency used in commercial transactions and a financial reference for pricing internationally traded goods.

Section Two: The Role of Technological Advancement and Its Applications in Military and Security Control

Technological development in the military field is among the areas that attract the greatest attention from both advanced and less-developed states. Many experts have argued that a major reason for the collapse of the Soviet Union was the Soviet leadership's concentration on the military sector, especially after U.S. claims of achieving superiority in space. This pushed the Soviet Union to devote considerable technological capacity to the development of an advanced missile project intended to narrow the gap with the United States in the context of what became known as the "Star Wars" initiative. The effort consumed extensive financial resources and redirected attention toward military development at the expense of other economic sectors. This contributed to the acceleration of the Soviet Union's collapse and the fall of the Eastern bloc. Despite this experience, the military domain remains one of the fields most dependent on technological and digital advancement. In the age of artificial intelligence, experts and observers expect warfare to become more advanced and more destructive as the world enters a technological revolution whose ultimate limits remain unknown.

First: Space and Satellite Technology and the Transformation of Military Conflict Management

The emergence of satellites, remote-sensing networks, and space-based communication systems has fundamentally changed the nature of warfare and the management of armed conflicts. Human resources and conventional military equipment are no longer the sole decisive standards of military superiority. Control over data and information collection, strategic planning, and the digital and technological domain has become a central measure of power.

The United States and its allies were among the first states to employ technological and digital capabilities in rapid military campaigns in several regions. They were able to achieve objectives quickly and effectively, as seen in Yugoslavia (1999), Iraq (1991 and 2003), Afghanistan (2001), and in the monitoring of field developments in Libya and Syria. Technological superiority enabled major armies to dismantle the air-defense, command, and control systems of Third World countries before the start of conventional ground or air operations.¹

¹ Sami Al-Manshawi, *Contemporary Military Technology and Digital Warfare Strategies* (Lebanon: Oueidat Publications, 2019), p. 112.

Second: Control of Global Cybersecurity and the Development of Espionage and Intelligence Methods

The Western strategic approach did not stop at military control. It also moved toward penetrating state security, undermining stability, and weakening internal cohesion. The West went beyond direct military confrontation and sought control over the cyber domain of states and institutions in Third World countries. Intelligence agencies in major powers developed highly advanced intrusion, counter-intrusion, and espionage software, including Pegasus-type spyware and zero-day exploits.

Such software can be used to create backdoors in operating systems and primary servers on which Third World countries depend. This allows advanced states to monitor government activity, conduct surveillance against leaders and officials, and extract resources and information without conventional military force. As a result, the traditional concept of regional or sovereign security becomes increasingly detached from practical reality.¹

The West has also been able to disrupt the security systems of Third World countries. This was clearly manifested in the policy of "creative chaos" in Arab states, where cyber penetration played a major role in destabilization. This contributed to severe and tragic collapse in countries such as Libya, Syria, Yemen, and Sudan, while other states have yet to recover from its destructive effects. Attempts have also been made to fragment the social fabric of states and demonize political regimes, as is currently occurring in Iran and other countries, with the aim of bringing them down from within and dismantling their social structures.

Section Three: The Emergence of Artificial Intelligence and the Future of International Conflict

Artificial intelligence is one of the most important variables to emerge at the global level. Following the digital revolution brought about by the Internet, the world entered another highly significant phase: the age of artificial intelligence. John McCarthy, who first introduced the term, defined it as "a means of making a computer, a computer-controlled robot, or a program think intelligently in the same way intelligent humans think. Artificial intelligence is achieved by studying how the human brain thinks, how humans learn, decide, and act while attempting to solve a problem, and then using the results of this study as a basis for developing intelligent programs and systems."²

Avron Barr and Edward Feigenbaum, in *The Handbook of Artificial Intelligence*, define it as "a branch of computer science concerned with designing intelligent computer systems; that is, systems that display characteristics associated with intelligence in human behavior."³

First: The Rise of China and Its Intense Competition with the United States

The international digital arena is no longer an exclusively U.S.-dominated domain. Recent decades have witnessed the substantial rise of the People's Republic of China, which has taken

¹ Omar Khalil, *Cybersecurity and National Sovereignty in the Age of Malicious Software* (Jordan: Dar Al-Fikr Al-Mu'asir, 2021), p. 134.

² Yahya Ibrahim Dahshan, "Criminal Liability for Artificial Intelligence Crimes," *Journal of Sharia and Law*, No. 82, Egypt, April 2020, pp. 109-110.

³ Rachida Hashemi and Abdelwahab Miliani, "The Conceptual Framework of Artificial Intelligence," *Al-Turath Journal*, Vol. 14, No. 2, Algeria, June 2024, p. 50.

advantage of technological progress and mobilized its material and knowledge resources to achieve self-sufficiency and then pursue international leadership.

China has succeeded in transforming its economy into the second-largest economy in the world and is considered a candidate to lead the global economy in the coming years. This position has been supported by the integration of digital technologies across productive sectors and by the growth of major companies such as Huawei, Tencent, and Alibaba. China's strategy has emphasized early engagement with artificial intelligence, the development of independent algorithms, and the processing of Big Data.¹

Second: Artificial Intelligence as a New Standard in the Comprehensive Power Equation

Artificial intelligence forms the core of a new generation of cyber-domain weapons. Its exceptional ability to process billions of data points within fractions of a second, predict the behavior of software systems, generate code, respond automatically to attacks, and launch complex autonomous attacks has made AI the most effective and lethal weapon of the modern era.

State power is no longer measured only by gross domestic product or by the number of tanks and aircraft a country possesses. The decisive criterion has become the scale of its supercomputing infrastructure, advanced algorithms, data-processing centers, and the quality of its human resources specialized in programming and artificial intelligence.²

Section Four: Implications of Technological Control for Third World Countries

First: Cyber Exposure and the Theft of Sovereign Data

The most serious problem facing Third World countries lies in their structural lag behind the technological and artificial intelligence revolution. They have largely remained consumer societies that depend on ready-made Western or Chinese solutions and software. Importing these systems without possessing their source code leaves their cybersecurity completely exposed.

Sensitive data belonging to Third World countries, including citizens' civil records, health data, financial systems, geographical maps, and military plans, have become stored and accessible on servers and in data banks located in advanced states or owned by transnational technology companies subject to the laws of those states.³

Second: Comprehensive Dependence and the Alienation of Economic and Value Systems

The consequences of digital and artificial intelligence superiority in the countries of the Global North are not limited to the military and security sphere. They extend to all areas of life in Third World countries:

1. **Economic dependence:** Linking banking, production, and commercial sectors in developing countries to international digital platforms places these economies at the direct mercy of monopolistic digital corporations and the powers that supply the technology.

2. **Cultural and value alienation:** Artificial intelligence algorithms and social media platforms function as engineered tools for shaping public opinion and directing social

¹ Mohamed Al-Sayed Hassan, U.S.-Chinese Strategic Competition in Advanced Technology (United Arab Emirates: Emirates Center for Strategic Studies and Research, 2022), p. 67.

² Khaled Al-Shami, Artificial Intelligence and the Future of Power in International Relations (Lebanon: Arab Institution for Studies and Publishing, 2023), p. 150.

³ Fatima Al-Zahra Ben Ahmed, "The Dependence of Southern Countries in the Digital Age and Its Impact on National Security," Journal of Law and Human Sciences, University of Djelfa, Vol. 15, No. 2, Algeria, 2022, p. 205.

behavior. They are used to impose Western values and cultural patterns and to weaken local national identities in Third World countries through hybrid warfare and fifth-generation warfare.¹

Conclusion

The foregoing shows that control over digital technologies and artificial intelligence has become a basic determinant of state power and international hegemony in the twenty-first century. This has generated intense competition among advanced states seeking to control the global landscape. At the same time, the failure of Third World countries to keep pace with technological and digital advancement and artificial intelligence has deepened the digital divide and technological inequality between the Global North and the Global South. It has also increased the dependence of Third World countries and placed their cyber and national security in a state of complete exposure and paralysis. This is especially evident where these countries rely almost entirely on foreign software and applications without developing domestic tools, reducing national sovereignty to a largely theoretical concept that lacks effective protection in practice.

Third World countries should therefore invest in human capital by modernizing school and university curricula and giving priority to technological sciences, programming, artificial intelligence, and cybersecurity. This should not come at the expense of the social sciences and humanities, which also play an important role in preparing and advancing society.

These countries should also establish local cloud and data-storage centers to keep sovereign, institutional, and private data within national borders and protect them from external penetration and control. They should encourage open-source software, localize technology, and enact effective legislation based on national or open-source solutions while reducing direct dependence on closed, ready-made foreign software. Regional groupings and South-South integration should also be strengthened to create a basis for cooperation among Third World and developing countries. Such cooperation can support shared cybersecurity networks and the exchange of expertise in confronting technological challenges, monopolistic cyber hegemony, and Western dominance.

References

Books

1. Khaled Al-Shami, *Artificial Intelligence and the Future of Power in International Relations*, Lebanon: Arab Institution for Studies and Publishing, 1st ed., 2023.
2. Sami Al-Manshawi, *Contemporary Military Technology and Digital Warfare Strategies*, Lebanon: Oueidat Publications, 1st ed., 2019.
3. Abdelrahman Bouzid, *Cyber Hegemony and the Penetration of Value Systems in Third World Countries*, Algeria: Dar Al-Umma for Printing and Publishing, 1st ed., 2021.
4. Abdelkader Mohamed, *International Relations in the Digital Age: From Geopolitics to Geo-Cyber Politics*, Egypt: Dar Al-Nahda Al-Arabiya, 1st ed., 2018.
5. Omar Khalil, *Cybersecurity and National Sovereignty in the Age of Malicious Software*, Jordan: Dar Al-Fikr Al-Mu'asir, 1st ed., 2021.
6. Mohamed Al-Sayed Hassan, *U.S.-Chinese Strategic Competition in Advanced Technology*, United Arab Emirates: Emirates Center for Strategic Studies and Research, 2022.

¹ Abdelrahman Bouzid, "Cyber Hegemony and the Penetration of Value Systems in Third World Countries," Algeria: Dar Al-Umma for Printing and Publishing, 2021, p. 94.

7. Osama Al-Husseini, Artificial Intelligence and an Introduction to the Lisp Language, Lebanon: Dar Al-Ratib Al-Jami'iyya.

Periodicals and Journals

1- Ibrahim Al-Ali, "The International Monetary System and the Weapon of Digital Sanctions," International Politics, No. 210, Al-Ahram Center for Political and Strategic Studies, Cairo, 2020.

2- Abdelrahman Bouzid, "Cyber Hegemony and the Penetration of Value Systems in Third World Countries," Algeria: Dar Al-Umma for Printing and Publishing, 2021.

3- Fatima Al-Zahra Ben Ahmed, "The Dependence of Southern Countries in the Digital Age and Its Impact on National Security," Journal of Law and Human Sciences, University of Djelfa, Vol. 15, No. 2, Algeria, 2022.

4- Rachida Hashemi and Abdelwahab Miliani, "The Conceptual Framework of Artificial Intelligence," Al-Turath Journal, Vol. 14, No. 2, Algeria, June 2024.

5- Yahya Ibrahim Dahshan, "Criminal Liability for Artificial Intelligence Crimes," Journal of Sharia and Law, No. 82, Egypt, April 2020.

Websites

1- Russell Hotten, "What Is the SWIFT Global System, and Why Is the West Divided over Excluding Russia from It as Punishment?" BBC Arabic, 25 February 2022:

<https://www.bbc.com/arabic/world-60524465>

Foreign-Language References

Books

Rowley, J. E., The Basics of Information Technology, Clive Bingley, London, 1988.