



Cyber Power: The Nature of Actors and Types of Conflict

Omrane Dalila Batoul Manal *

Ziane Achour University OF Djelfa
(Algeria)Laboratory of Democratic
Development and Human Rights
dalila.omrane@univ-djelfa.dz

Received: 26/12 /2025

Accepted: 16/03 /2026

Published: 31/03 /2026

Abstract:

Digital technological impact has transformed the concept of power in international conflict, as cyberspace has become a new arena for wars, changing the concept of national security to focus on protecting the state's information infrastructure. States have shifted from traditional threats to conflicts with different tools and means, and new actors. This shift has been reflected in the practice of power, as conflict has become focused on technological competition, opening alternative forms of warfare that require multilateral alliances, thus increasing the interconnectedness of technology and security.

Keywords: cyberspace , cyber power, power, conflict, actors , international relations.

Introduction :

The impact of digital technology on the transfer of power in international relations has radically transformed the concept of conflict in cyberspace. Many states have entered the cyber domain, considering it a new arena for international conflicts where power is practiced through advanced technological capabilities. In this context, reliance on technology has altered the nature of war, shifting it from the traditional level to a new level of threats, where conflicts now depend on means and methods fundamentally based on modern technology.

* Corresponding author□



In this study, we will try to answer the following problem

What is the nature of conflict in cyberspace?

THE FIRST TOPIC : The Concept of Power in International Relations

The concept of military power alone is no longer a sufficient criterion for determining the power of states. The development witnessed in international relations has produced new determinants and multiple types of power that are not limited to the military aspect only. Some countries have emerged with strong global standing despite lacking the elements of traditional military power, while others have appeared with military power but suffer from economic weakness.

This difference indicates that the definition of power is no longer limited to the military dimension, but now includes other, more comprehensive factors. Among the most prominent of these factors are economic power, the natural or produced resources, strategic geographic location, population, geographical area, as well as cultural values and the nature of political leadership. These determinants, taken together, contribute to classifying states based on the interaction of these elements and their influence on the international stage.

Power in international relations is a fundamental determinant for understanding state behavior. It is defined as "the ability to influence the behavior of others to achieve desired outcomes," and it is a fundamental basis for understanding a state's potential and ability to be influential in international politics¹.

Power refers to the ability of an international actor to use tangible and intangible resources and assets to influence the outcomes of events in the international system in a way that enhances its convictions within the system.²

International relations researchers often classify power into:

FIRST REQUIREMENT: Hard Power

Hard power, which refers to a state's military capabilities, technological advancements, and economic power, and is based on coercion and compulsion.

¹ - Obaid Al-Halimi, The Evolution of the Concept of Power in Contemporary International Relations, Arab Democratic Center, <https://democraticac.de/?p=67404>

² -Ahmed Elsayed Khairallah, The impact of the development of the concept and elements of power on the transformations of the international system, Journal of Financial and Commercial Research, Volume 20, Issue 03, (2019), p. 160.



Military power occupies the central position within this category of power. Military power is determined by two aspects: one aspect relates to its sources, which can be provided by the country's area, population, and the size of its army; and the other aspect relates to employing these resources in a way that serves the field use of military power (ground forces, air forces, navies)

SECOND REQUIREMENT: Soft Power

Soft power, based on the priority of persuasion and focusing on elements of cultural strength, values, and political achievements, creates a powerful attraction that leads to compliance. In this sense, soft power is the attractive force capable of winning people over with argument and drawing them towards shared values, justice, and a shared contribution to achieving those values.³

THIRD REQUIREMENT: Smart Power

Smart power is neither a distinct concept from soft and hard power, nor an entirely new one. It is a concept based primarily on the two powers, but with conditions and strategies that take into account a number of requirements. Joseph Nye mentioned this concept in 2003 to combat the myth that soft power produces an effective foreign policy. It refers to a strategy that successfully combines hard and soft power in different contexts. It is available to actors, both states and non-state actors. The concept of smart power comes in the process of power transformation, as some states have many sources of power but fail to transform them into outputs that benefit the state.

Joseph Nye emphasizes the importance of the context in which smart power strategies are used. Since power is the ability to influence the behavior of others to get what you want, the tools of smart power are coercion and attraction, and neither can be relied upon in isolation from the other.⁴

FOURTH REQUIREMENT: Cyber Power

Cyber power this concept is linked to the tremendous technological development of our time. Cyber power refers to possessing technological knowledge and the ability to use it by exploiting cyberspace to influence events occurring across operational environments. Cyberspace is employed to achieve

³ - Boubaker Al-Jawhari, Power Transformations and Conflict Resolution *On the Feasibility of Military Power*, Khaled Al-Hassan Studies and Research, No. 12, (2018), p. 59.

⁴ - Maryam hazzam, The New Concept of Power in International Relations in the Age of Big Data. Master's T hesis. Department of Political Science, University of Guelma, 2021, p. 25



other advantages that may fall under the categories of hard, soft, or smart power. According to Joseph Nye, this type of power is associated with three actors: the state, non-state actors, and individuals. This power also requires several factors, including advanced information infrastructure, interconnected electronic devices, software, and trained skills.⁵

Joseph Nye defined cyber power as: the ability to achieve desired results through the use of electronically linked information resources in cyberspace and to control activities, computers, and information infrastructure related to cyberspace; that is, the ability to use cyberspace to create advantages for the state and to influence events related to other operational environments through cyber tools⁶.

THE SECOND TOPIC : Actors in Cyberspace

Recent decades have witnessed fundamental changes in the structure of international relations, abandoning some of its traditional assumptions that considered the state the primary and pivotal actor in this field. Political and social movements, along with terrorist organizations, have become influential actors on the international stage. Furthermore, multinational corporations and global non-governmental organizations are playing an increasing role in shaping international dynamics and driving events on the global stage.

FIRST REQUIREMENT: State Actors

In this context, state actors refer to states and governments. Based on their material, structural, human, and legal capabilities, the state is considered a pivotal actor in managing cyberspace. The state must control the cyberspace field to extend its influence and achieve its aims in this cyber domain, where it is competed with by many other actors, which may even threaten its interests.

According to Joseph Nye's classification of power types (soft power and hard power), cyber capabilities are considered part of soft power. Therefore, countries have sought to develop their cyber capabilities. Major powers such as the United States, China, Britain, and Russia are no longer the only ones possessing advanced

⁵- Obaid Al-Halimi, op.cit.

⁶- Ehab Khalifa, *Electronic Power: How Can the State Manage Its Affairs in the Internet Age?*, Arab Publishing and Distribution, Cairo, 2017, p. 24



cyber capabilities; new countries have emerged, such as India, Australia, Indonesia, South Korea, Iran, and Turkey.⁷

SECOND REQUIREMENT: Non-State Actors

Non-state actors has a significant role in cyberspace, both in terms of interaction and influence. This is due to the low cost of accessing this field, the absence of obstacles, and the ease of obtaining the necessary tools from the Internet, which facilitates launching attacks on targets directed at states or non-state actors.

1- Non-Governmental Organizations (NGOs):

NGOs are among the actors that carry out cyberattacks. However, they lack the resources and capabilities of a state, and their attacks are limited to relatively low-value targets such as websites, aiming for minimal profit before detection and legal action. This context also includes both ordinary and criminal organizations, the latter of which operate exclusively in the cyberspace such as the Japanese Yakuza or the Asian Triads, which engage in money laundering, extortion, financial fraud, hacking, industrial espionage, and employing programmers to create threats and sell information online through data brokerage and other activities.⁸

2- Multinational Corporations

Multinational corporations are fundamental players in cyberspace because they possess resources and power that surpass those of some countries, and they do not lack the legitimacy to practice power, which is the exclusive domain of states. The servers of companies like Google, Facebook, Microsoft, Apple, and Amazon have enormous financial resources and branches in many countries around the world, allowing them control over proprietary code. This provides them with greater financial resources than many governments. These companies can easily influence in cyber conflicts due to the low cost of investment and the difficulty of identifying their identities. Furthermore, these companies influence national

⁷ - Amin Boutata, Cyber Warfare in International Relations: Concept and Phenomenon, Master's Thesis in International Relations, University of Skikda, 2022, p. 53 .

⁸ - Abdelkader Bougazi, Cyber Deterrence: An Approach to Nature, Actors and the Constraints of International Law, Algerian Journal of Law and Political Science, Volume 10, No. 01 (2025), p. 863



economies, societal cultures, and trends, as seen in the conflict between Google and China over content, and also in the Cambridge Analytica scandal, where Facebook user data was leaked to Cambridge Analytica, which was used to benefit the campaign of former US President Donald Trump.⁹

3-Terrorist Groups

Terrorist groups are among the most prominent international actors, especially after the events of September 11th. They exploit cyberspace for recruitment, mobilization, propaganda, fundraising, and volunteering. They also attempt to gather information about military targets, weapons use to train new recruits, although they have not yet reached the stage of launching a full-scale cyberattack on national infrastructure.¹⁰

4. Individuals

Individuals are important actors in cyberspace, possessing the ability to revolutionize information. This revolution then becomes a field used by states themselves (for example, Julian Assange founded WikiLeaks, a website for publishing classified documents. The site receives information and documents from around the world from those who wish to expose unethical behavior in governments and corporations¹¹).

THE THIRD TOPIC: Transformation in the Nature of Conflict

Current technological developments, embodied in the communications and information revolution and the advancement of military industries, have led to a radical reshaping of the ways in which relations between states and other actors are conducted. While conflict over "territories" (land, sea, and air) persists, the emergence of new spaces, most notably cyberspace, and the increasing

⁹ -Mohammed Akram Mohsen, *Cybernetics..... The nature - characteristics - actors - strategic dimensions*, Hammurabi Journal, No. 43 (2022), p. 398.

¹⁰ -Hassan Hani Mahmoud, *The Impact of Cyber Threats on National Security: A Case Study of Malaysia*; 2015-2022, available at <https://democraticac.de/?p=90955>

¹¹ -Mohammed Akram Mohsen, *The use of cyber power by non-state actors and its impact on national security*, Institute Journal, Issue 15 (2023), p. 542.



interconnectedness between traditional territories and technological developments, have produced more diverse and complex patterns in the arena of conflict.

FIRST REQUIREMENT: Factors contributing to the spread of cyber conflict

Two main factors have contributed to the spread of conflict in cyberspace, thus opening the way for the emergence of cyber wars, namely:

1- The perspective of war has changed radically, as it has moved from the pattern of wars between states to among peoples. The purpose of war in the past was to destroy the enemy, either by occupying its land or seizing its resources. New wars, however, primarily target the will and choices of societies. Peoples then appeared to have a pivotal importance in this new pattern of warfare, whether it was the population targeted on the battlefield, public opinion in the state waging the war, or public opinion at the regional and international levels.

With this change, the objectives of war became less material and focused more on the psychological and propaganda aspect, especially with live news, audio, and visual coverage of events as they happen via websites and satellite channels, and the weakening of the control of ruling regimes over the attitudes of their citizens.

2-The emergence of conflicts with local and international dimensions, as the outbreak of internal conflicts in the post-Cold War era, as well as the nature of the international context of cyberspace, helped to provide a suitable environment for integrating marginalized groups and forces into international politics, and creating a network of alliances of support or opposition with a broad international scope, either on the basis of human rights values, or ethnic or religious affiliations.¹²

SECOND REQUIREMENT: Characteristics of Cyber Conflict

Cyber conflict differs from traditional conflict in several ways, including:

¹² -Bouatamine Lakhdar, Cyber Warfare: Backgrounds, Levels, and Future Implications. Journal of Legal and Political Research. Volume 07, Issue 01 (2022), p. 971.



1. A virtual arena of conflict: Virtual conflict does not have a specific geographical location but is characterized by open arenas where opposing parties clash across cyberspace.

2.Tools of conflict: These are electronic tools that utilize data, information, and computer systems.

3. Due to the nature of cyber weapons, the value of deterrence no longer functions as it does in traditional conflicts, whether with conventional or nuclear weapons. In other words, the value of deterrence as a military strategy has diminished and no longer has a clear impact.

4.Cyber conflict has increased the chances of asymmetric warfare, and accordingly, less powerful countries have become capable of launching attacks on larger and more powerful countries. With the expansion and ease of access to cyberspace, the scope of cyber conflicts has broadened, the number of attackers has increased, and the struggle between different actors has shifted towards acquiring protection and defense tools and developing offensive cyber capabilities. The aim is to gain power, superiority, and dominance, fostering competition for control, innovation, and information, thereby increasing power, influence, and leverage at both the local and international levels.¹³

THEIRD REQUIREMENT: Objectives of Cyber Conflict

1- Cyber conflict of a political nature may take a military form where offensive and defensive capabilities are used in cyberspace with the aim of disrupting information systems, networks, and infrastructure. This type of conflict involves the use of cyber weapons by actors within the information society, or through cooperation with other powers, to achieve political objectives.

2-A cyber conflict of a soft nature, the conflict over obtaining information, influencing ideas and waging psychological and media warfare, and this is done through leaking information and using it through media platforms, which affects the nature of international relations, such as the role played by WikiLeaks in international diplomacy.

3-Cyber conflict over technological advancement, where this type of cyber conflict takes on a competitive character regarding gaining the upper hand in the technological advancement race, stealing economic and scientific secrets, and may

¹³ -Shaimaa Marouf Farhan, The Transformation in the Concept of Conflict: A Study in Cyber Warfare, Political Issues Journal, Issue 75 (2023), p. 501.



extend to attempts to control the internet,, website addresses, control information, and work to breach national security.

4-Cyber conflict over information: With the difficulty of gathering information, engaging in cyber warfare, or distinguishing between political and criminal use, cyberspace appears to be a more suitable environment for information conflicts. It contributes to supporting the ability of state security agencies, or even different groups, to form a global network of agents without direct involvement. In addition, the low cost, ease of communication, and difficulty of traditional monitoring of electronic interactions make it an attractive element for the use of cyber weapons and their deployment to achieve political and military objectives.¹⁴

Conclusion

The form of power in international relations has transformed, with alternatives to direct warfare emerging through innovative technological strategies. These conflicts have highlighted the urgent need for alliances involving governments, international organizations, and the private sector, adapting to new forms of social organization and complex patterns of socio-political conflict. In this context, the digital revolution has provided radical changes in the form of wars, their tools, and their impact on military apparatuses and actors, prompting the adoption of new approaches to understanding the dynamics of conflict and its impact on the international relations.

Bibliography List setting:

Books;

-Ehab Khalifa, *Electronic Power: How Can the State Manage Its Affairs in the Internet Age?*, Arab Publishing and Distribution, Cairo, 2017.

Articles :

¹⁴ -Bou El-Tamine Lakhdar, op.cit, p. 972.



- Abdelkader Bougazi, Cyber Deterrence: An Approach to Nature, Actors and the Constraints of International Law, Algerian Journal of Law and Political Science, Volume 10, No. 01 (2025).

-Ahmed Elsayed Khairallah, The impact of the development of the concept and elements of power on the transformations of the international system, Journal of Financial and Commercial Research, Volume 20, Issue 03, (2019).

-Boubaker Al-Jawhari, Power Transformations and Conflict Resolution *On the Feasibility of Military Power*, Khaled Al-Hassan Studies and Research, No. 12, (2018).

- Bouatamine Lakhdar, Cyber Warfare: Backgrounds, Levels, and Future Implications. Journal of Legal and Political Research. Volume 07, Issue 01 (2022).

- Mohammed Akram Mohsen, Cybernetics..... The nature - characteristics - actors - strategic dimensions, Hammurabi Journal, No. 43 (2022).

- Mohammed Akram Mohsen, The use of cyber power by non-state actors and its impact on national security, Institute Journal, Issue 15 (2023).

- Shaimaa Marouf Farhan, The Transformation in the Concept of Conflict: A Study in Cyber Warfare, Political Issues Journal, Issue 75 (2023).

memory:

- Amin Boutata, Cyber Warfare in International Relations: Concept and Phenomenon, Master's Thesis in International Relations, University of Skikda, 2022.

- Maryam hazzam, The New Concept of Power in International Relations in the Age of Big Data. Master's Thesis. Department of Political Science, University of Guelma, 2021.

Websites:

- Obaid Al-Halimi, The Evolution of the Concept of Power in Contemporary International Relations, Arab Democratic Center,
<https://democraticac.de/?p=67404>

-Hassan Hani Mahmoud, The Impact of Cyber Threats on National Security: A Case Study of Malaysia; 2015-2022, available at
<https://democraticac.de/?p=90955>