Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Cybersecurity and the Reshaping of International Security: An Analytical Study of Its Levels and Political-Strategic Dimensions

Yacine Hachouf [1], Abdelmalik Medjadba [2], Mohamed Messika [3], Benali Khalil [4]

[1] University of Bechar-Tahri Mohamed (Algeria). Laboratory of Law and Development. E-mail: hachouf.yacine@univ-bechar.dz

[2] University of Bechar-Tahri Mohamed (Algeria). Laboratory for Researchand Studieson Human and Society Issues. E-mail: abdelmalik.medjadba@univ-bechar.dz

[3] University of Bechar-Tahri Mohamed (Algeria). Laboratory of Law and Development.E-mail: messika.mohamed@univ-bechar.dz

[4] University of Djelfa- Ziane Achour (Algeria). Laboratory for Development, Democracy, and Human Rights in Alger. E-mail k.benali@univ-djelfa.dz

ARTICLE INFO

Received: 12 Apr 2025

Revised: 21 Sep 2025

Accepted: 20 Nov 2025

ABSTRACT

This study examines cybersecurity as a central pillar of contemporary international security, highlighting its individual, institutional, and international dimensions, and its role in reshaping global power and dominance. It explores cybersecurity as a tool of foreign policy, digital deterrence, informational hegemony, and the geopolitical influence of major technology corporations, alongside structural critiques emphasizing digital dependency and the North-South technological gap. The study concludes that cybersecurity is no longer merely a technical concern but a strategic function linking politics, economics, law, and human dimensions. Effective governance at national, regional, and international levels is essential to ensure a secure and stable digital space, balancing sovereignty, freedom, and digital development.

Keywords: : Cybersecurity, Digital Sovereignty, Information Hegemony, Major Tech Companies, Cyber Justice

Introduction

The contemporary international system is undergoing profound transformations due to the digital revolution, which has made cyberspace a fundamental pillar in the structures of the state, society, and economy. With the growing reliance on technology, so-called cyber threats have emerged—intangible, transnational threats that challenge traditional concepts of sovereignty and deterrence.

Today, cybersecurity has become one of the major determinants of national security and global hegemony, as the competition among major powers has shifted from military and economic domains to the informational sphere. Power is increasingly measured by the ability to control data and information flows (Clarke & Knake, 2019).

In this context, cyberspace represents a new battleground that transcends physical geography, where non-state actors can exert strategic effects equivalent to conventional warfare. Consequently, cybersecurity is no longer merely a technical matter but a political and strategic issue that directly impacts power balances within the international system.

The "WannaCry" (2017) and "SolarWinds" (2020) attacks revealed the vulnerability of global infrastructures and demonstrated that cybersecurity has become a prerequisite for international

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

stability (Healey, 2021). This underscores the importance of treating cybersecurity as a central variable in international relations, encompassing multiple levels and intersecting technical, political, economic, and legal dimensions.

Cyberspace has thus become an open arena of conflict, where state interests intertwine with those of non-state actors, and the boundaries between internal and external security increasingly blur. Accordingly, the study revolves around a central research question:

How do the different levels of cybersecurity affect strategic and political stability in the contemporary international system?

Building on the research problem concerning how different levels of cybersecurity affect strategic and political stability within the contemporary international system, there arises a need to develop explanatory hypotheses that guide the analysis and help clarify the nature of the relationships between these levels and the geopolitical dynamics generated by the digital space. Cybersecurity, as a multidimensional phenomenon, does not operate in isolation or within a single framework; rather, it manifests through a complex interaction among individual actors, institutions, states, and major powers. Consequently, formulating precise hypotheses is essential to examine the extent to which these interactions reshape the international system and to interpret emerging patterns of digital hegemony and competition.

Based on this, the following hypotheses can be formulated:

Hypothesis 1: The diversification of cybersecurity levels—from individual and institutional to international—leads to a restructuring of the global security architecture, with each level uniquely influencing the political and strategic stability of states.

Hypothesis 2: The utilization of cybersecurity as a tool for geopolitical hegemony by major powers contributes to creating a more fragile international environment and reshapes strategic balances according to who possesses digital superiority.

In light of the research problem and these guiding hypotheses, the study seeks to dissect the multiple dimensions of cybersecurity as one of the most significant variables redefining contemporary international security. With the rapid transition to digital space, cybersecurity is no longer merely a technical matter; it has become an interpretative framework for understanding political and strategic interactions among actors within the international system. Accordingly, the study aims to clarify cybersecurity concepts, identify its main analytical levels, and explore its role as a tool for geopolitical hegemony, thereby enabling a deeper understanding of the shifts in power and influence in the digital era. Additionally, the study seeks to highlight how these levels impact international stability and to anticipate the potential future trends arising from the evolution of cyberspace on the structure of the global system.

Given the nature of the research problem and the complexity of cybersecurity, intertwined with political and strategic dimensions, the study adopts a **descriptive-analytical methodology**, considered the most suitable approach for understanding the phenomenon in its multifaceted context. The descriptive aspect allows for a precise presentation of core concepts and identification of cybersecurity dimensions, while the analytical component facilitates the interpretation of relationships between its various levels and their influence on international stability. This methodology also provides a framework to examine cybersecurity as a mechanism for redistributing geopolitical power through the analysis of real-world models and scenarios involving state behavior and international actors in cyberspace. Consequently, the descriptive-analytical approach enables the construction of a

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

comprehensive perspective linking conceptual understanding with explanatory insights, thus serving the study's objectives and providing a deep comprehension of the transformations shaping the international system amid growing cyber threats and opportunities.

The study is structured around **two main axes**, namely:

Axis 1: The Concept of Cybersecurity and Levels of Analysis

Axis 2: Cybersecurity as a Tool for Geopolitical Hegemony

Axis 1: Concept and Levels of Analysis:

1- Definition of Cybersecurity and the Concept of Cyberspace

Cybersecurity is one of the contemporary concepts that has acquired a multidimensional character, encompassing technical, political, and strategic aspects. Technically, it is defined as "a set of measures and technologies aimed at protecting digital systems, networks, and data from attacks and breaches," while its political significance extends beyond the technical dimension to include all aspects related to the protection of national interests in the digital domain.

Cyberspace refers to the digital environment emerging from the interaction of information systems, communication networks, and data. It is a space not constrained by geographical boundaries, making it an open arena for all actors—states, corporations, or individuals—to exercise influence, launch attacks, or safeguard their interests. Kello (2017) described it as the new infrastructure of contemporary international relations, where control over information has become one of the primary sources of power.

From a political perspective, cybersecurity is directly linked to the concept of digital national sovereignty, which denotes a state's ability to control its information space and protect critical data from external interference. This dimension raises a fundamental debate regarding whether cyberspace represents an extension of traditional state sovereignty or a novel domain outside conventional legal and political jurisdictions.

Understanding the position of cybersecurity within the international system requires a **multilevel perspective** that integrates technological and political analysis, as well as national and collective security considerations. Cybersecurity is not merely an "additional dimension" of international relations; it has become a cornerstone of global security and an indicator of power balances in the twenty-first century.

2-Levels of Analysis in Cybersecurity

Cybersecurity constitutes a multi-level system, in which individual, institutional, and international dimensions are intertwined, making it impossible to understand from a single perspective. As emphasized in contemporary international relations literature, modern security phenomena—unlike traditional military threats—transcend the state as a sole actor and encompass individuals, corporations, transnational organizations, and even algorithms and intelligent systems, which now play a quasi-independent role in managing information flows and automated decision-making.

In this context, cyberspace emerges as an open domain where political authority intersects with technical capability and economic power, rendering cybersecurity a hybrid field in which concepts of sovereignty, responsibility, accountability, and deterrence overlap within a framework that is difficult to regulate under traditional international law. This qualitative shift in the nature of actors and tools of influence has also redefined notions of threat and risk. Danger is no longer limited to direct military

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

attacks; it manifests through data breaches, information manipulation, or disruption of critical services, with profound political, social, and strategic consequences for state stability and security (Taddeo & Floridi, 2018).

Based on this perspective, cybersecurity can be analyzed across **three interconnected levels**:

Individual Level: Humans as Both a Weak and a Strong Link

The human element constitutes a cornerstone in the cybersecurity ecosystem, representing simultaneously the most targeted point of vulnerability and the most decisive source of strength in building digital protection. On one hand, most cybersecurity incidents indicate that human error—such as weak passwords, falling for phishing schemes, or mishandling links and files—remains one of the primary gateways for breaches. On the other hand, individual awareness and digital literacy form the first line of defense against cyber threats, as individuals possess the capacity to distinguish between safe and malicious content, adhere to protective measures, and contribute to cultivating responsible collective behavior within institutions and society.

In this context, the individual transforms from being merely a "user" into a key security actor, making cybersecurity as much a cultural and behavioral matter as it is a technical one. Based on this perspective, cybersecurity can be analyzed across **three interconnected levels**:

a- Humans at the Heart of Cyberspace:

Individuals occupy a central position within the structure of cyberspace, manifesting both as active users of digital technologies, direct targets of cyberattacks, and, in some cases, potential sources of threats themselves. Cyber risks no longer stem solely from the complexity of technical systems; the human element has become the pivotal factor in the success or failure of attacks. Contemporary literature shows that a significant proportion of cyber incidents result from unsafe human behaviors, such as falling victim to phishing schemes, poor password management, or limited awareness of digital security policies (Hadnagy, 2020).

However, reducing humans to merely a "weak link" oversimplifies their true role. Individuals remain the most capable actors in enhancing the resilience of cybersecurity systems through advanced digital awareness, adoption of preventive behaviors, and promotion of a security-conscious culture within institutions and communities. In this sense, the individual transforms from a passive technology user into a central security actor, rendering cybersecurity as deeply connected to cultural, educational, and cognitive dimensions as it is to technical infrastructure.

The centrality of humans in cyberspace reflects a structural shift in contemporary threats: technological capability alone is no longer sufficient to ensure security. Investment in "cognitive security" has become essential for achieving digital stability. Modern attacks increasingly rely on social engineering techniques that target human perception before attacking systems, making individual awareness a hidden battleground between attacker and defender. Furthermore, the rise of remote work, online banking, and social media has expanded individuals' exposure to threats, making cybersecurity a concern that directly impacts citizens' daily lives. Consequently, integrating digital literacy into educational policies, developing continuous institutional training programs, and enhancing individual responsibility in data and privacy protection are essential, positioning individuals as active partners in achieving collective digital security.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

b-Psychological and Behavioral Dimension of Cybersecurity:

From a political and behavioral perspective, cybersecurity constitutes a complex domain where the psychological intersects with the political, authority intersects with knowledge, and technology intersects with social behavior. It goes beyond protecting systems or data to influence individuals' perceptions and guide their decisions in digital spaces. In this context, states and institutions aim to shape "desired" digital behaviors through a mix of incentives and deterrence tools, known as behavioral engineering approaches, which draw on cognitive psychology, behavioral economics, and social compliance theories.

Behavioral engineering manifests in the design of guided digital environments using "choice architecture," where user interfaces and security policies are structured to nudge individuals toward safer decisions without direct coercion. Mechanisms such as instant alerts, two-factor authentication, and enforced password updates are not merely technical measures but political-behavioral tools intended to reshape user habits and establish sustainable "security routines" in digital life.

This dimension reveals a profound transformation in the nature of power in the digital age. Authority is no longer exercised solely through direct orders or traditional coercive control, but through the organization of the choice environment itself. Here, cybersecurity becomes a new form of digital social governance, redefining freedom, privacy, and responsibility within a technological space governed by algorithms and pre-designed structures. Thus, cybersecurity is not merely a technical or procedural matter but reflects a deep transformation in governance and behavior management in the digital public sphere, making it an integral part of modern power and soft authority tools in shaping societal awareness and conduct.

c-Digital Citizenship and Digital Rights:

From a rights-based political perspective, cybersecurity is organically linked to the concept of digital citizenship, which denotes individuals' ability to exercise fundamental rights—such as freedom of expression, privacy, and access to information—within cyberspace without exposure to unlawful violations or surveillance. The digital domain is no longer neutral; it has become a central arena for exercising civil and political rights, making cybersecurity an issue that transcends technical protection to touch the core of the state-citizen relationship in the digital age.

This shift raises broad debates about the security-freedom equation, especially in contexts where cybersecurity policies are used to expand surveillance or restrict political and social actions under the guise of maintaining stability. Recent studies, including those by Deibert, highlight that some governments leverage digital security discourse to legitimize practices that exceed lawful oversight, thereby eroding the digital public sphere and turning it into a monitored and politicized space (Deibert, 2020).

In this framework, cybersecurity issues intersect directly with political and legal challenges, raising structural questions about the legitimacy of digital surveillance, the constitutionality of personal data collection, and the limits of state intervention in citizens' digital lives. The concept of digital sovereignty emerges as one of the most controversial aspects, reflecting states' attempts to assert control over data flows and digital infrastructure within their borders while balancing the protection of individual rights and freedom of cyberspace. Accordingly, in its rights-based dimension, cybersecurity is not merely a matter of protective measures but a genuine test of a state's legal maturity and its ability to achieve a delicate balance between security imperatives and freedom in the digital age.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Institutional Level: Organizations as Security Actors in Cyberspace :

The institutional level represents a central axis in the analysis of cybersecurity, as organizations—whether governmental institutions, private companies, or international organizations—are no longer merely users of digital technologies but have become primary security actors in cyberspace. Today, organizations manage critical digital infrastructures, control vast flows of data, and possess technical and organizational capabilities that place them in a decisive position to either safeguard or compromise digital security. In this context, cybersecurity is no longer an internal technical issue confined to IT departments; it has become a strategic function embedded within institutional governance structures, where considerations of national security intersect with the requirements of organizational continuity, reputation management, and public trust. Consequently, organizations now represent central nodes in the cybersecurity network, contributing to the reshaping of power and responsibility balances within the digital domain at both national and international levels.

a. Public and Private Institutions as Cybersecurity Guardians:

At the institutional level, cybersecurity constitutes a cornerstone of modern governance in both public and private sectors. The modern state no longer monopolizes security, as major corporations (such as Google, Amazon, and Microsoft) possess cybersecurity capabilities that surpass those of some states, whether in protection, data analysis, or even executing counterattacks (Carr, 2016).

This transformation has given rise to a new model of state-private sector relations, based on partnership rather than monopoly. Government institutions increasingly rely on private companies to secure energy grids, communication networks, banking systems, and administrative infrastructures. The so-called "cooperative cybersecurity model" emerges as a new institutional framework for managing digital risks, based on shared responsibilities, threat information exchange, and joint response mechanisms between government agencies and technology providers. In this context, cybersecurity is no longer a purely sovereign domain but has become a hybrid field in which the state and private sector share the roles of "digital guardians." This raises profound questions regarding the limits of legal responsibility, the legitimacy of private cyber power, and the future of state monopoly over security in the digital age.

b. Digital Governance and Risk Management:

Within organizations, cybersecurity is part of a broader system known as Information Technology (IT) Governance. This system concerns defining roles and responsibilities, establishing security policies, and assessing potential risks. Studies indicate that institutions with clear and documented structures for managing digital risks exhibit greater flexibility and resilience, enabling them to respond swiftly to attacks or disruptions and recover from crises without significant impact on operational continuity or organizational reputation.

Clear policies, regular testing procedures, and ongoing staff training enhance an organization's ability to adapt to evolving threats, transforming cybersecurity from a set of technical tools into a strategic element of institutional capacity. Thus, cybersecurity within organizations is not merely a technical obligation but a vital lever for good governance and institutional sustainability, ensuring operational security and efficiency even in the face of sophisticated and evolving cyberattacks.

c. Political Institutions and Cybersecurity as a Tool for Legitimacy:

From a political science perspective, cybersecurity extends beyond its traditional role of protecting information systems to become a strategic tool for reinforcing institutional legitimacy. The ability to protect citizens and institutions from digital threats is no longer merely technical but serves as an

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

indicator of a state's competence in managing its resources and safeguarding its critical interests, directly affecting public trust in government.

States that demonstrate readiness and effective capacity to counter cyberattacks—through robust infrastructure, proactive policies, or public awareness and training programs—gain additional credibility and reinforce their legitimacy. Conversely, failures in securing digital infrastructure can trigger political trust crises, undermining the state's credibility both domestically and internationally.

In this context, cybersecurity becomes part of a new social contract in the digital age, where state effectiveness is measured not only by traditional military protection but by its ability to safeguard citizens' informational space and ensure data privacy. Nye (2021) notes that cybersecurity has become a benchmark for government performance, testing a state's ability to adapt to complex digital environments, manage accelerated risks, and establish reliable standards for digital security. This political-security dimension reflects a transformation in the concept of sovereignty, where the capacity to protect digital information constitutes an integral part of state authority and legitimacy. The digital citizen thus becomes a partner in evaluating state effectiveness, reshaping the relationship between ruler and ruled in the digital era, and positioning cybersecurity not merely as a defensive tool but as a means to build trust, stability, and political legitimacy.

International Level: Cybersecurity as a New Global System :

Cybersecurity is no longer merely a technical or domestic issue; it has emerged as a new global system in which security, politics, and the digital economy intersect. In cyberspace, states, multinational corporations, and international organizations interact continuously, making the management of digital threats and challenges a shared responsibility that transcends traditional boundaries of national sovereignty. This transformation positions cybersecurity as a fundamental element in reshaping the international balance of power, as the ability to protect critical infrastructures, manage data, and control information flows has become a benchmark of influence and global authority. Understanding cybersecurity at the international level therefore requires a comprehensive approach that includes the development of international legal frameworks, cyber norms, multilateral alliances, and information sharing and coordination among global actors to counter transboundary attacks and threats. In this sense, cybersecurity becomes a pivotal factor in shaping international stability and the relationships between major powers.

a. The Emergence of Cybersecurity as an International Security Issue:

At the international level, cybersecurity has gradually shifted from a technical, domestic concern to a core component of inter-state relations. It is now classified among non-traditional security issues alongside environmental, health, and food security, reflecting the broadening scope of threats in the contemporary international system. Cyberspace is no longer a neutral communication domain; it has become a contested arena where strategic national interests intersect and new forms of power and influence are exercised.

Cyberattacks targeting Iran's nuclear program, which became prominent since 2010, marked a pivotal turning point in states' understanding of this threat. These operations demonstrated that targeted digital campaigns could inflict strategic damage comparable, in some cases, to conventional warfare, whether by disrupting critical infrastructures or weakening sensitive national capabilities. This shift has prompted a reevaluation of traditional concepts of deterrence and conflict, as cyber tools have become an integral part of the power arsenal of major states.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

In response, the United Nations initiated international pathways aimed at establishing responsible behavior norms in cyberspace, through expert groups and UN working bodies tasked with developing standards to regulate state conduct and mitigate escalation risks. However, achieving a comprehensive international agreement has remained stalled due to structural disagreements among major powers, particularly regarding differing interpretations of "digital sovereignty," the limits of national control over cyberspace, and the legitimacy of "preventive cyber defense" and offensive cyber operations. Consequently, cybersecurity has emerged as one of the most prominent arenas of strategic competition in the international system, reflecting a profound transformation in the nature of conflict and cooperation among states.

b. The Rise of Cyber Diplomacy:

In the past decade, international relations have witnessed the emergence of cyber diplomacy as a new approach to managing interactions between states in cyberspace, amid escalating cyber threats and increasing global reliance on digital infrastructures. Cyberspace is no longer a neutral technical domain but has transformed into a political–legal arena requiring specialized diplomatic tools for negotiation, confidence-building, and digital crisis management. In this context, several global powers have established dedicated units and institutional structures; for instance, the European Union created a specialized cyber diplomacy unit in 2017, while France launched its "National Strategy for Cyber Diplomacy" in 2018 to frame cyber practice within a logic of cooperation and escalation prevention. The EU further enhanced its instruments through the **EU Cyber Diplomacy Toolbox (2019)**, aimed at developing collective response mechanisms and political coordination against cyber threats.

Through cyber diplomacy, states seek to achieve three strategic objectives that reflect a transformation in the nature of traditional diplomatic practice:

1. **Preventing international cyber conflicts** by promoting dialogue, transparency, and information exchange regarding cyber doctrines and capabilities, thereby reducing misunderstandings and unintentional escalation.

2. **Developing legal and ethical norms** governing the use of digital power, in the absence of a binding international legal framework regulating cyber operations.

3. **Supporting global digital development within a collective security framework**, ensuring that cyberspace is not monopolized by technologically advanced states but serves as a platform for international cooperation and digital equity, thereby enhancing global stability and fairness.

Accordingly, cyber diplomacy represents a structural shift in the international system, where discussions on security are increasingly intertwined with debates on technology, information, and digital sovereignty.

c. Interactions among Major Powers: The United States, China, and Russia:

Cyberspace has become one of the most critical arenas of strategic competition among major powers, where the ability to control the digital domain carries symbolic and practical significance comparable to possessing conventional military capabilities. Competition is no longer confined to nuclear arms races or geographical influence but extends to controlling global digital infrastructure, defining acceptable norms of conduct in cyberspace, and shaping international digital governance standards. In this context, cyber policies are integral components of the security doctrines and grand strategies of the United States,

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

China, and Russia, reflecting differing visions of the international system and the future of sovereignty in the digital age.

The United States has adopted an offensive–defensive approach known as **"Defend Forward"**, which aims to neutralize cyber threats at their source before they reach U.S. territory or affect critical infrastructure. This strategy reflects a shift in deterrence from reactive to proactive, emphasizing anticipatory and digital containment measures (U.S. DoD, 2021). The U.S. approach treats cyberspace explicitly as a theater of operations requiring continuous presence and rapid intervention capability.

In contrast, China embraces the principle of **"cyber sovereignty"**, granting the state comprehensive control over information flows within its digital borders and rejecting any form of external interference in its information infrastructure. This principle aligns with a broader strategy to leverage digital tools to enhance China's global economic and political influence, notably through the **"Digital Silk Road"**, which seeks to construct cross-border communication networks and digital infrastructures under Chinese technological influence (Liu, 2020).

Russia has developed an approach centered on **"information warfare"** as a core element of its security doctrine, integrating cyberattacks with media disinformation campaigns and psychological operations aimed at undermining adversaries' stability and internal cohesion. Recent events indicate that this low-cost, high-impact Russian model has been employed in multiple contexts, notably influencing the information environment during crises in Ukraine in 2014 and 2022 (Connell & Vogler, 2017).

This divergence in cyber strategies illustrates that the digital domain is no longer a secondary competitive field but a principal arena for reshaping power balances, where each major power seeks to assert its vision of sovereignty, security, and legitimacy in the emerging digital international order.

d. Cyberspace as a New Field of Power and Hegemony:

From a critical perspective in international relations and global political economy, cybersecurity can be seen as a new domain for reproducing patterns of global hegemony in digitally sophisticated and subtler forms than traditional mechanisms. Hegemony is no longer exercised solely through military superiority or direct economic control; it now manifests in the domination of data flows, communication platforms, cloud infrastructures, and operating systems that form the backbone of the global digital economy. In this context, major technology corporations in Western countries dominate a large portion of global data centers, cloud services, and social networks, granting them unprecedented capacity to influence markets, shape behaviors, and control the pathways of digital knowledge. In contrast, developing countries often remain consumers rather than producers of technology, resulting in structural marginalization.

This structural imbalance opens the door for new critical approaches, including the concept of **"Cyber Justice"**, which advocates for the equitable redistribution of digital opportunities, narrowing the technological gap between the Global North and South, and building a fairer global system for managing cyberspace (Couldry & Mejias, 2019). This approach situates cybersecurity not merely as a defensive matter but within a broader framework concerning equitable access to technology, collective control over digital knowledge, and preventing cyberspace from becoming a tool for perpetuating digital dependency.

The various levels of cybersecurity—individual, institutional, and international—do not operate in isolation but constitute a complex interactive network in which these dimensions interweave within a non-linear structure of influence and interdependence. A simple cyber incident targeting an individual

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

or organization can rapidly escalate into a transnational diplomatic or political crisis, while geopolitical tensions between states may translate into targeted digital attacks on civilian infrastructures, such as power grids, communication systems, or financial sectors. This structural interconnection compels political science to rethink the very concept of security, which should not be reduced to a "protective shield" or traditional deterrent. Instead, security must be reconceptualized as a comprehensive ecological system requiring a delicate balance between technology, politics, and human factors, and demanding integrative approaches that account for overlapping interests, multiple actors, and the evolving nature of threats in the digital era.

Axis Two: Cybersecurity as a Tool for Geopolitical Hegemony :

I.From Nuclear Deterrence to Cyber Deterrence:

The transition from the nuclear deterrence model to cyber deterrence represents a qualitative shift in contemporary strategic thought, where deterrence no longer relies solely on the threat of catastrophic retaliation but increasingly focuses on preventing an adversary from achieving their objectives from the outset by raising the cost of attack and reducing the likelihood of success. While nuclear deterrence during the Cold War was based on the principle of **"Mutually Assured Destruction"**, cyber deterrence operates on a different logic, emphasizing defensive hardening, institutional resilience, and operational continuity—essentially denying the adversary the strategic impact intended by a cyberattack rather than focusing primarily on punitive retaliation. Lindsay (2013) notes that the effectiveness of cyber deterrence is closely linked to a state's ability to develop resilient systems capable of absorbing shocks and maintaining operations while minimizing damage.

In this context, the United States has embraced this shift in deterrence logic within its modern defense doctrine. It no longer relies solely on passive defense policies but has adopted a proactive approach, engaging in **forward defense** within cyberspace to thwart threats before they reach U.S. territory or critical infrastructure (U.S. DoD, 2021). This approach reflects the American understanding that the cyberspace environment differs fundamentally from the nuclear domain in terms of attribution difficulties, attack velocity, and the multiplicity of actors, making reliance solely on post-attack retaliation insufficient for effective deterrence. Consequently, cyber deterrence represents a new model of international security based on a combination of technical prevention, defensive deployment, and risk management rather than the traditional logic of deterrence based on the threat of total retaliation.

II. Digital Sovereignty and Information Hegemony:

Contemporary states seek to extend their sovereignty over their informational space, treating it as a new domain of sovereignty comparable in importance to territorial, air, or maritime domains. However, this endeavor generates structural tension between national security imperatives and the principles of internet freedom and information flow, as noted by Chander & Lê (2015). The more states tighten control and surveillance over their digital infrastructure, the greater the concerns about undermining digital rights, restricting freedom of expression, and turning cyberspace into an extension of political control tools.

In this context, the United States exercises a form of indirect digital hegemony through networks of major technology companies that control a significant portion of the global internet infrastructure, social media platforms, and cloud services, granting it strategic influence beyond traditional state boundaries. Despite its rhetoric in support of an "open internet," this model reflects a form of soft hegemony based on control over technological standards, data flows, and the global digital economy.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

China, on the other hand, has pursued a "sovereign internet" model, relying on the relative isolation of its national network from the global digital space, through advanced regulatory and technical systems and centrally controlled local infrastructure. This model is not confined to domestic application; Beijing actively exports it to Global South countries via cross-border digital infrastructure initiatives, offering an alternative approach that prioritizes political stability and digital sovereignty over the concept of an open internet.

Similarly, Russia seeks to develop its own "sovereign internet" model by establishing a national infrastructure capable of operating independently of Western networks in emergencies or conflicts, consolidating state control over internal and external data flows. This approach reflects a Russian recognition that reliance on a global infrastructure dominated by Western companies and data centers represents a strategic vulnerability in times of geopolitical tension.

Consequently, cyberspace shifts from being a global arena for knowledge exchange to a sovereignty-driven field of contestation where considerations of security, freedom, and influence intersect. Each major power aims to reshape the internet according to its strategic interests, deepening the international divide between the open internet model and the sovereign internet model, while maintaining the underlying tension between protection requirements and user rights.

III. Tech Giants as Geopolitical Actors:

Tech giants such as Google, Meta, and Amazon have emerged as new geopolitical actors, exerting political and economic influence that often surpasses the capacity of states themselves to control information and data flows (Keen, 2015). These companies are no longer merely commercial enterprises; they control the essential infrastructure of the global digital space, including massive data centers, cloud computing services, and social media platforms that now constitute the global public sphere.

Their influence extends to indirect impacts on political decision-making within states, through political lobbying and the establishment of technical standards that effectively become informal international rules. The algorithms of these platforms are no longer neutral; they actively shape public agendas, guide political discourse, and influence public opinion, granting these companies unprecedented power over the political and social stability of states.

Furthermore, these companies control the most strategic resource of the digital age: big data, which represents a new form of power. Mastery over the data of billions of individuals allows them to predict social and political behaviors, target communities with precision messaging, and even influence elections and the trajectories of democratic processes in some countries.

From an international relations perspective, this reality has reshaped the concept of sovereignty. The state is no longer the sole actor managing cyberspace; "transnational private powers" have emerged, imposing their agendas and rules on governments. In this sense, these companies resemble "informal digital states" managing significant portions of the global digital sphere outside traditional democratic accountability, thereby reinforcing a new pattern of cross-sovereignty digital hegemony (Keen, 2015).

IV. Cybersecurity and Foreign Policy:

Cybersecurity has become an integral tool of foreign policy, with digital attacks serving as an extension of traditional diplomacy and a form of "soft" warfare that is highly effective in practice. States no longer rely solely on military power or economic pressure; they now use cyberspace to influence adversaries,

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

disrupt institutions, and shape domestic and international public opinion. Digital attacks have thus become a new form of smart power in international relations.

In the Middle East, Israel and Iran adopt hybrid strategies that combine cyber operations, digital espionage, disinformation campaigns, and the political use of cyberattacks within regional power struggles. This approach adds a new dimension to traditional deterrence, as regional balances are no longer measured solely by missile or tank counts but also by a state's ability to penetrate, disrupt, and exert influence through cyberspace.

This evolution redefines sovereignty and borders in foreign policy, as digital attacks transcend traditional geopolitical boundaries without leaving clear physical evidence, enabling "low-cost, high-impact" conflicts. Consequently, states increasingly integrate cybersecurity into their diplomatic strategies—through implicit threats, digital alliances, or the development of cyber deterrence capabilities—making cyberspace a central arena of twenty-first-century geopolitical competition.

V. The Economic Dimension:

The economic dimension of cybersecurity is one of the most sensitive and impactful aspects of the contemporary international system. Data has effectively become the "oil of the twenty-first century," a strategic resource as valuable as energy or natural resources. States and corporations now compete not only in traditional markets but also for control over big data, information flows, and the ability to analyze and convert this data into tangible economic and political power.

Technological rivalries between China and the United States—especially regarding Huawei and TikTok—illustrate this advanced competition for digital hegemony. The confrontation now extends beyond tariffs and economic sanctions to areas such as artificial intelligence, semiconductors, and communications infrastructure (Segal, 2017). These disputes reflect a shift in the global economic center of gravity from traditional industries to platform economies and high technology, making cybersecurity an inseparable part of the economic national security of major powers.

Control over undersea cables, the backbone of the global internet, represents a crucial, often unacknowledged geopolitical battleground, as most global data flows traverse these networks. Similarly, 5G networks have become a critical arena of competition due to their role in connecting vital infrastructure, smart cities, and military and economic systems. This control represents a new form of "digital geopolitical geography," where boundaries are drawn not only on paper maps but also through fiber optic routes, communication towers, and satellite networks (Kaplan, 2021). Thus, cybersecurity has become a regulatory framework for global economic competition, intersecting commercial interests with calculations of power and influence at both regional and international levels.

VI. Structural Critique of Cybersecurity:

The structural critique of cybersecurity examines the deep-rooted dimensions of digital hegemony and the unequal relationships between major tech companies, advanced states, and developing countries. From this perspective, cybersecurity is not merely a tool for protecting systems and infrastructure; it functions as a means to justify Western digital colonialism and reinforce epistemic centrality. Advanced states and major technology corporations dominate digital knowledge production, data management, and the setting of technological standards, which become effectively global by default. Scholars such as DeNardis (2020) and Couldry & Mejias (2019) argue that this dominance entrenches the digital divide between the Global North and South, rendering developing countries primarily technology consumers rather than producers, deepening digital dependency and limiting national sovereignty in cyberspace.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Structural critique also highlights how power is reproduced through cyberspace, with the notion of security exploited to justify surveillance, restrict access to information, and control global digital markets. In this framework, cybersecurity extends beyond system protection to serve as a political and strategic instrument for consolidating influence and epistemic control. This phenomenon is sometimes described as "multi-level digital hegemony," where technical, political, and economic power intersect within a single digital space.

Based on this analysis, critical theorists advocate for a "cyber justice" approach, aimed at redistributing digital opportunities more equitably and empowering developing states and marginalized communities to access technology and knowledge. This approach seeks to balance relationships between global actors and limit the use of cyberspace as a tool for domination. Consequently, cybersecurity is framed not merely as a defensive measure but as a strategic political and social issue that reflects the structural interplay of power, sovereignty, and knowledge in the contemporary digital world.

Conclusion:

Today, cybersecurity has emerged as a fundamental pillar of modern international security and a critical domain that intertwines both conflict and cooperation. Digital threats are no longer confined to states or institutions; they now encompass individuals, corporations, and transnational organizations, reflecting a profound transformation in the nature of security and international relations in the twenty-first century. At a time when global power and influence are being tangibly redistributed among major states, cybersecurity poses unprecedented ethical and legal challenges, touching upon the core of sovereignty, freedom, and political legitimacy, while raising critical questions regarding the responsibilities of both public and private actors.

Addressing this complex reality requires a comprehensive, multi-level approach that accounts for technical, political, strategic, and human dimensions, while integrating the interactions of individuals, institutions, and states within cyberspace. From this perspective, building a more stable and just international system necessitates global digital governance capable of balancing security with freedom, and sovereignty with openness, recognizing that any weakness at one level can rapidly escalate into an international crisis. It also demands the strengthening of national and regional capacities, alongside the development of multilateral cooperation mechanisms, to ensure that cyberspace becomes a space for development and stability rather than conflict and domination.

This vision is accompanied by a set of strategic recommendations aligned with multi-level analysis, outlining actionable measures:

A. National Level:

1. Integrate cybersecurity into the comprehensive national security doctrine to ensure coherence between defense, economic, and political policies.

2. Develop modern national legislation regulating data usage and privacy protection, while enhancing accountability and transparency.

3. Invest in defensive artificial intelligence systems to counter evolving cyberattacks and enable rapid, precise threat analysis.

4. Establish national cybersecurity councils comprising representatives from the public and private sectors to coordinate policies and formulate contingency plans.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

B. Regional Level:

1. Create regional centers for information coordination, expertise exchange, and technical services in cyberspace.
2. Strengthen cooperation among Arab and African states in training, digital research, and the development of shared infrastructure.
3. Adopt a unified regional legal framework to combat cybercrime, similar to the Budapest Convention, ensuring effective and consistent enforcement.

C. International Level:

1. Promote a comprehensive United Nations cybersecurity treaty that establishes international norms of behavior in cyberspace and safeguards the rights of all actors.
2. Involve developing countries and non-state actors in global policy-making to ensure equitable representation and greater transparency.
3. Support UN initiatives to establish an International Cybersecurity Council under the auspices of the Security Council to monitor attacks, prevent escalation, and enhance inter-state cooperation.
4. Expand collaboration between the private sector and governmental institutions to develop shared cybersecurity standards, ensuring alignment with technical, legal, and political requirements at the international level.

Adopting these recommendations across national, regional, and international levels represents a decisive step toward redefining cybersecurity as an integral component of comprehensive international security. It enhances the capacity of the global community to address complex digital challenges in a balanced manner, reconciling the protection of national interests with respect for digital rights, while fostering a secure and stable cyberspace for all actors.

Bibliography:

[1] Abdulrahman, A. (2022). Cybersecurity Capacity in Developing Nations: Bridging the Global Digital Divide. Journal of Cyber Policy, 7(1), 34–51.
[2] Brundage, M., Avin, S., Clark, J., & Toner, H. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford University Press.
[3] Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.
[4] Chander, A., & Lê, U. P. (2015). Data Nationalism. Emory Law Journal, 64(3), 677–739.
[5] Connell, M., & Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis & Solutions.
[6] Couldry, N., & Mejias, U. (2019). The Costs of Connection: How Data Is Colonizing Human Life. Stanford University Press.
[7] DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.
[8] EU Cyber Diplomacy Toolbox. (2019). Council of the European Union Document 6122/19. Brussels.
[9] FireEye. (2021). M-Trends 2021: Insights into Cyber Threats. FireEye Inc.
[10] Healey, J. (2021). A Fierce Domain: Conflict in Cyberspace, 1986 to 2021. Cyber Conflict Studies Association.

[11] ITU. (2023). Global Cybersecurity Index Report 2023. International Telecommunication Union.
[12] Kaplan, F. (2021). Dark Territory: The Secret History of Cyber War. Simon & Schuster.
[13] Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404.
[14] Liu, F. (2020). Digital Silk Road: China's Technological Strategy for Global Influence. Routledge.
[15] Madise, Ü., & Martens, T. (2019). E-Governance and Cybersecurity in Estonia: A Model for the World. Government Information Quarterly, 36(4), 101–113.
[16] Mansour, K. (2020). Iran's Cyber Capabilities and Regional Strategy. Middle East Policy, 27(3), 89–103.
[17] Maurer, T. (2021). Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press.
[18] Nye, J. S. (2021). Do Morals Matter? Presidents and Foreign Policy from FDR to Trump. Oxford University Press.
[19] Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
[20] Segal, A. (2017). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.
[21] Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
[22] Tikk, E. (2020). International Cyber Law and Policy. NATO Cooperative Cyber Defence Centre of Excellence.
[23] UNDP. (2022). Digital Security and Human Development Report. United Nations Development Programme.
[24] U.S. Department of Defense. (2021). Cyberspace Operations Strategy. Washington, D.C.
[25] Valeriano, B., & Maness, R. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press.
[26] World Bank. (2022). Building Digital Resilience in Developing Countries. World Bank Group.
[27] Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.