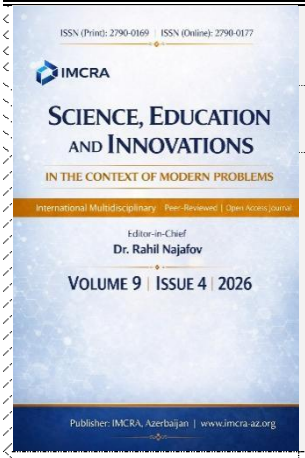


Science, Education and Innovations in the Context of Modern Problems
Issue 4, Vol. 9, 2026

RESEARCH ARTICLE

The Transformation of International Security Systems in the Age of Cybersecurity: A Multidimensional Analysis of Threats, Actors, and Strategic Competition

Tamta Kodua
PhD Student
Caucasus International University
Georgia
Email: tamta.kodua@ciu.edu.ge ; https://orcid.org/0000-0002-4563-7131

Keywords Cybersecurity; International Security; Cyber Warfare; Hybrid Threats; Digital Geopolitics; Cyber Governance; Strategic Competition; Critical Infrastructure

Abstract

In the context of rapid digital transformation, cybersecurity has emerged as a central component of contemporary international security, fundamentally reshaping the structure and dynamics of global power relations. The increasing dependence of states, institutions, and societies on digital infrastructures has amplified the scale, complexity, and transnational nature of cyber threats, positioning cyberspace as a critical domain of geopolitical competition in the 21st century. This study aims to examine the evolving relationship between international security systems and cybersecurity within the framework of a changing world order. It analyzes how the transition from a traditional, state-centric security paradigm to a multidimensional and networked security environment has altered the nature of threats, actors, and strategic responses. The research focuses on the role of state and non-state actors, the growing importance of public–private partnerships, and the challenges posed by attribution, governance, and regulatory frameworks in cyberspace. Methodologically, the study adopts a qualitative analytical approach, drawing on comparative analysis, theoretical frameworks in international relations, and selected case-based evidence from leading global actors. It integrates perspectives from security studies, geopolitics, and cyber governance to provide a comprehensive understanding of the contemporary cybersecurity landscape. The findings demonstrate that cybersecurity introduces a new layer of complexity into international security by blurring the boundaries between war and peace, civilian and military targets, and domestic and international domains. The study highlights the limitations of existing international legal and institutional frameworks, emphasizing the need for enhanced cooperation, norm development, and adaptive governance mechanisms. Furthermore, it underscores the strategic significance of cybersecurity in shaping geopolitical competition and influencing the balance of power in the digital age. The originality of this research lies in its integrated analysis of cybersecurity as both a technological and geopolitical phenomenon, offering a multidimensional perspective on its impact on international security systems. The study contributes to the growing body of literature by proposing a conceptual understanding of cybersecurity as a transformative force in the reconfiguration of global security architecture.

Citation

Kodua, T. (2026). The Transformation of International Security Systems in the Age of Cybersecurity: A Multidimensional Analysis of Threats, Actors, and Strategic Competition. *Science, Education and Innovations in the Context of Modern Problems, 9*(4), 1–11. https://doi.org/10.56334/sei/9.4.21

Received: January 04 .2025 | **Accepted:** March 19. 2026 | **Published Online:** April 04.2026

Introduction

The transformation of the international security system during the Cold War constitutes one of the most significant structural shifts in modern geopolitical history. Over approximately four decades, the bipolar international order evolved through distinct phases, reflecting changes in ideological competition, military capabilities, and global power distribution. These phases may be broadly categorized as follows: (1) 1945–1956, characterized by the consolidation of opposing security blocs; (2) 1957–1979, marked by ideological expansion and intensified geopolitical competition; and (3) 1980–1989, defined by systemic decline and the gradual emergence of alternative centers of power (Gaddis, 1997; Halliday, 1983).

In the initial phase, the international system was shaped by the establishment of mutually exclusive spheres of influence dominated by the United States and the Soviet Union. As Saul Bernard Cohen (2003) argues, this division was not merely ideological but also geographical, with the Soviet Union consolidating control over continental Eurasia, while the United States extended its influence across maritime domains. The institutionalization of these spheres through alliances such as NATO, the Warsaw Pact, SEATO, and CENTO reflected a strategic effort to contain opposing ideologies and secure geopolitical dominance (Brzezinski, 1992; Kissinger, 2014).

The concept of a "cordon sanitaire," implemented primarily by Western powers, represented a deliberate geopolitical strategy aimed at limiting Soviet expansion. This approach was reinforced through military alliances, economic aid programs, and political interventions, particularly in Europe and Asia (Cohen, 2003). Simultaneously, regional conflicts such as the Korean War, the Chinese Civil War, and the Indochina War served as critical arenas in which the broader ideological confrontation between capitalism and communism materialized (Westad, 2007). These conflicts not only reshaped territorial boundaries but also contributed to the stabilization of bipolar divisions by the mid-1950s.

The second phase of the Cold War was characterized by the increasing global projection of Soviet influence, facilitated by nuclear parity and ideological adaptability. Following the Soviet Union's acquisition of ballistic nuclear capabilities, the rigid bipolar structure began to exhibit greater flexibility, allowing for indirect competition across the Global South. The emergence of liberation movements, combined with the decline of European colonial empires, created opportunities for Soviet expansion into regions such as the Middle East, Africa, and Southeast Asia (Halliday, 1983; Gaddis, 1997). These regions, often described as "shatterbelts," became zones of persistent instability and conflict, where local dynamics intersected with global geopolitical rivalries (Cohen, 2003).

Recent historiographical developments have challenged traditional interpretations of the Cold War as a strictly bipolar confrontation dominated by superpowers. Instead, scholars emphasize the agency of regional actors and the significance of South–South interactions in shaping global political dynamics (Westad, 2007). This perspective highlights the complexity of international relations during this period, revealing that states in Latin America, Africa, and Asia were not merely passive recipients of superpower policies but active participants in the global system.

By the late Cold War period, structural transformations within the Soviet Union, particularly economic stagnation and political decline, contributed to a reconfiguration of global power. The rise of East Asia as a significant economic and geopolitical region, driven by Japan's economic expansion and the rapid development of newly industrialized economies such as South Korea, Taiwan, Hong Kong, and Singapore, introduced a new dimension to the international system (Arrighi, 2007). This shift signaled the gradual transition from a rigid bipolar order toward a more complex and interconnected global structure.

Methodology

This study employs a qualitative research design aimed at examining the relationship between cybersecurity and the transformation of international security systems. The research is based on a combination of theoretical analysis and comparative evaluation of existing literature in the fields of international relations, security studies, and cyber governance.

A systematic review of academic sources, including peer-reviewed journal articles, books, and policy reports, was conducted to identify key concepts, trends, and debates related to cybersecurity and global security dynamics. In addition, selected case-based examples (e.g., cyber incidents affecting critical infrastructure and state-level cyber operations) were used to support analytical interpretations.

The study adopts an interdisciplinary approach, integrating perspectives from political science, geopolitics, and information security. This approach enables a comprehensive understanding of cybersecurity as both a technological and geopolitical phenomenon influencing contemporary international security systems.

Literature Review

The evolution of international security has been extensively examined within the frameworks of classical realism, neorealism, and liberal institutionalism. Traditional security paradigms, particularly those articulated by Kenneth Waltz (1979),

conceptualize the international system as anarchic, where states act as primary actors seeking survival through power balancing. Within this framework, the Cold War is often cited as a quintessential example of a stable bipolar system, where the distribution of power between the United States and the Soviet Union contributed to strategic equilibrium (Gaddis, 1997).

However, contemporary scholarship has increasingly challenged the sufficiency of state-centric approaches in explaining modern security dynamics. The rise of globalization, technological innovation, and transnational threats has necessitated a broader analytical perspective. Scholars such as Joseph Nye (2017) argue that power in the digital age extends beyond military capabilities to include cyber power, information control, and technological dominance. This shift reflects a transition from traditional hard power to a more complex interplay of hard, soft, and smart power.

Cybersecurity has emerged as a central theme in this evolving discourse. Early studies on cyber conflict, such as those by Rid (2013), questioned whether cyber war constitutes a fundamentally new form of warfare or merely an extension of existing strategic practices. In contrast, Kello (2017) emphasizes the transformative potential of cyber capabilities, arguing that cyberspace introduces a new strategic environment characterized by ambiguity, speed, and low barriers to entry.

The role of non-state actors has also received significant attention in the literature. Valeriano et al. (2018) highlight how cyber operations are no longer monopolized by states, as private actors, hacker groups, and transnational networks increasingly participate in cyber activities. This diversification of actors challenges traditional hierarchies of power and complicates governance mechanisms. Similarly, Carr (2016) underscores the importance of public–private partnerships in national cybersecurity strategies, given that much of the critical infrastructure is owned and operated by private entities.

Another key strand of literature focuses on the governance and normative dimensions of cybersecurity. Dunn Cavelty (2013) argues that cybersecurity discourse is shaped by threat perceptions that influence policy decisions and institutional responses. The development of international norms and legal frameworks, although still limited, reflects ongoing efforts to regulate state behavior in cyberspace (Klimburg, 2017).

Furthermore, scholars have examined the intersection between cybersecurity and democratic governance. Buckland et al. (2015) highlight the tension between security measures and the protection of human rights, particularly in relation to surveillance and data privacy. This tension underscores the need for governance models that balance security imperatives with democratic principles.

Recent research also emphasizes the concept of hybrid warfare, where cyber operations are integrated with informational, economic, and political strategies to achieve strategic objectives without direct military confrontation (Valeriano et al., 2018). This approach reflects a broader transformation in the nature of conflict, where the boundaries between war and peace are increasingly blurred.

Despite the growing body of literature, significant gaps remain. In particular, there is a need for integrative approaches that combine geopolitical, technological, and governance perspectives to provide a comprehensive understanding of cybersecurity's role in international security. This study seeks to address this gap by offering a multidimensional analysis of cybersecurity within the context of a changing global order.

Discussion

The findings of this study provide important insights into the transformation of international security systems in the digital age, highlighting both continuities and disruptions in relation to traditional security paradigms. While the Cold War system was characterized by relatively stable power structures and clearly defined actors, the contemporary cybersecurity environment introduces a level of complexity that challenges existing theoretical frameworks.

One of the key points of discussion concerns the shift from a state-centric to a multi-actor security environment. The increasing role of non-state actors, including private corporations and cybercriminal networks, fundamentally alters the distribution of power within the international system. This shift supports the arguments of Valeriano et al. (2018) and Carr (2016), who emphasize the decentralization of authority in cyberspace. However, it also raises questions about accountability and the effectiveness of governance mechanisms, particularly in situations where responsibility for cyber incidents cannot be clearly assigned (Najafov, 2025).

Another critical issue relates to the limitations of traditional deterrence strategies. The concept of deterrence, which was central to Cold War stability, is less effective in cyberspace due to the challenges of attribution and the asymmetrical nature of cyber threats (Nye, 2017). This finding aligns with Lindsay (2013), who argues that cyber operations often operate below the threshold of conventional warfare, making it difficult to apply traditional deterrence models. As a result, states must explore alternative approaches, including resilience-building and cooperative security frameworks.

The discussion also highlights the growing importance of public–private partnerships in cybersecurity governance. The reliance on private actors for the management of critical infrastructure necessitates new forms of collaboration between governments and the private sector. While such partnerships can enhance security capabilities, they also introduce governance challenges related to transparency, trust, and the distribution of responsibilities (Dunn Cavelty & Wenger, 2020).

Furthermore, the study underscores the tension between security and human rights, which remains a central challenge in the development of cybersecurity policies. Measures aimed at enhancing security, such as surveillance and data collection, can conflict with fundamental rights, including privacy and freedom of expression (Buckland et al., 2015). This tension highlights the need for normative frameworks that ensure accountability and protect democratic values while addressing security concerns.

Another important aspect of the discussion is the integration of cybersecurity into broader geopolitical competition. Cyber capabilities are increasingly used as tools of strategic influence, enabling states to achieve political and economic objectives without engaging in direct military confrontation (Kello, 2017). This development reflects the emergence of hybrid forms of conflict, where cyber operations are combined with informational and economic strategies to shape global power dynamics.

At the same time, the study reveals that existing international legal and institutional frameworks remain insufficient to address the complexities of cyberspace. Although various initiatives have been undertaken to establish norms of responsible behavior, their voluntary nature limits their effectiveness. This finding suggests the need for stronger international cooperation and the development of binding agreements that can enhance stability and predictability in the cyber domain (Klimburg, 2017).

Finally, the discussion points to the necessity of revising existing theoretical approaches in international relations. Traditional theories, while still relevant, are insufficient to fully capture the multidimensional nature of cybersecurity. An interdisciplinary approach that integrates insights from political science, information technology, and legal studies is essential for understanding the evolving security landscape.

Theoretical Foundations of the Cold War System

The Cold War international system can be understood through the lens of structural realism, particularly the framework developed by Kenneth Waltz (1979). According to neorealist theory, the international system is inherently anarchic, lacking a central authority capable of enforcing rules and maintaining order. Within this context, states act primarily in pursuit of survival, leading to the formation of power balances that shape global stability.

Despite efforts to establish a cooperative international order through institutions such as the United Nations, the coexistence of competing ideological systems undermined the effectiveness of these mechanisms. The absence of enforcement capabilities within the UN structure resulted in a system dominated by power politics, where the United States and the Soviet Union functioned as the primary actors (Kissinger, 2014).

The bipolar structure of the Cold War is widely regarded as a stabilizing factor in international relations. As Gaddis (1997) argues, bipolarity reduced uncertainty and limited the number of actors capable of initiating large-scale conflict, thereby decreasing the likelihood of systemic instability. Furthermore, the concept of mutually assured destruction (MAD) played a critical role in preventing direct military confrontation between the superpowers, reinforcing a strategic equilibrium based on deterrence (Nye, 2017).

In addition to military considerations, ideological moderation contributed to the stability of the system. Although both superpowers maintained universalist ideological ambitions, they gradually adapted their policies to accommodate the realities of coexistence. This resulted in the emergence of informal norms governing international behavior, including respect for spheres of influence and the avoidance of direct confrontation (Gaddis, 1997; Halliday, 1983).

However, this stability was not absolute. The Cold War was characterized by cyclical patterns of tension and détente, reflecting shifts in political leadership, economic conditions, and strategic priorities. Periods of reduced tension, such as the détente of the 1970s, were often followed by renewed competition and conflict, illustrating the dynamic nature of the international system (Halliday, 1983).

Transition Toward Contemporary Security Paradigms

While the Cold War provides a foundational framework for understanding modern international security, the emergence of new technological domains has fundamentally altered the nature of global threats. In particular, the rise of cyberspace as a critical arena of interaction has introduced unprecedented challenges for states and international organizations.

Cybersecurity has become a central component of contemporary security strategies, reflecting the increasing reliance of societies on digital infrastructure. Unlike traditional security threats, cyber threats are characterized by their transnational nature, anonymity, and asymmetry, making them difficult to detect, attribute, and counter (Kello, 2017; Rid, 2013). These

characteristics challenge conventional notions of sovereignty and complicate the application of existing international legal frameworks.

Moreover, the involvement of non-state actors, including private corporations, hacker groups, and transnational networks, has further blurred the boundaries between public and private security. As Carr (2016) notes, the growing importance of public–private partnerships in cybersecurity governance reflects the need for collaborative approaches to address complex and evolving threats.

The integration of cybersecurity into geopolitical competition has also transformed the strategic landscape of international relations. Cyber capabilities are increasingly viewed as instruments of power, enabling states to project influence, disrupt adversaries, and achieve strategic objectives without resorting to conventional military force (Lindsay, 2013; Valeriano et al., 2018). This shift underscores the need to reconsider traditional security paradigms and develop new theoretical frameworks capable of capturing the complexities of the digital age (Najafov, 2025).

At the same time, cybersecurity raises significant challenges for democratic governance, particularly in relation to issues of surveillance, privacy, and human rights. Efforts to enhance national security through digital monitoring and data collection must be balanced against the protection of civil liberties, highlighting the tension between security and freedom in contemporary societies (Dunn Cavelty, 2013; Buckland et al., 2015).

Toward a Multi-Dimensional Understanding of Cybersecurity

The evolving nature of cybersecurity necessitates a comprehensive and multi-dimensional analytical approach that integrates political, technological, and socio-economic perspectives. Unlike traditional security domains, cyberspace operates as a highly interconnected and decentralized environment, where actions in one region can have immediate and far-reaching global consequences (Singer & Friedman, 2014).

In this context, the role of international organizations and regulatory frameworks becomes increasingly important. Institutions such as the United Nations, NATO, and regional bodies have sought to develop norms and guidelines for responsible behavior in cyberspace, although their effectiveness remains limited by the lack of binding enforcement mechanisms (Klimburg, 2017).

Furthermore, the rapid pace of technological innovation continues to outstrip the development of policy and governance structures, creating a persistent gap between capability and regulation. This gap is particularly evident in areas such as cyber warfare, artificial intelligence, and critical infrastructure protection, where existing frameworks are often inadequate to address emerging risks (Kello, 2017).

In light of these challenges, it is essential to examine how the principles of international security can be adapted to the digital age, taking into account the unique characteristics of cyberspace and the diverse range of actors involved. This requires not only theoretical innovation but also empirical analysis of state behavior, institutional responses, and the broader socio-political implications of cybersecurity in the contemporary international system...

Building upon the structural stability of the Cold War system, the behavioral patterns of its principal actors further reinforced the relative equilibrium that characterized this period. As highlighted by John Lewis Gaddis (1986), the restrained strategic behavior of the United States and the Soviet Union played a crucial role in preventing direct military confrontation. This restraint was primarily grounded in the doctrine of nuclear deterrence and the concept of mutually assured destruction (MAD), which established a strategic environment in which the costs of full-scale war far outweighed any potential gains (Nye, 2017; Waltz, 1979).

In this context, both superpowers adopted a calculated risk-taking approach, engaging in indirect competition through proxy conflicts while avoiding direct confrontation. This strategic restraint contributed to the emergence of an informal set of norms governing international behavior. These norms included respect for established spheres of influence, limitations on the use of force, and the prioritization of stability over systemic transformation (Gaddis, 1997; Kissinger, 2014). The preservation of anomalies—such as the existence of politically divergent regimes within opposing spheres—further reflected the pragmatic adaptation of ideological positions to geopolitical realities.

Moreover, the Cold War system demonstrated a degree of internal flexibility, allowing for limited deviations within each bloc. The pursuit of strategic autonomy by European actors, particularly under leaders such as Charles de Gaulle, and the implementation of Ostpolitik by Willy Brandt, exemplify the capacity for intra-bloc differentiation without undermining the overall stability of the system (Halliday, 1983). Similarly, the Sino-Soviet split introduced a degree of multipolarity into an otherwise bipolar structure, highlighting the dynamic and evolving nature of global power relations (Westad, 2007).

At the same time, smaller states exercised agency by leveraging their positions within the bipolar system to maximize strategic benefits. Countries such as India and Egypt adopted balancing strategies, while others aligned more closely with one of the

superpowers to secure economic and military support (Brzezinski, 1992). This interaction between global and regional dynamics underscores the complexity of the Cold War system, which cannot be fully understood through a purely bipolar lens.

Despite the persistent tensions and periodic crises that defined the Cold War, the international system also exhibited a remarkable capacity for cooperation and institution-building. Initiatives such as the Baruch Plan, the Atoms for Peace program, and the Open Skies proposal illustrate the willingness of superpowers to engage in dialogue and pursue mechanisms aimed at reducing the risks of conflict (Gaddis, 1997). The development of arms control agreements, including the Treaty on the Non-Proliferation of Nuclear Weapons, further demonstrates the ability of the international system to establish regulatory frameworks in the face of existential threats (Kissinger, 2014).

The Helsinki Accords and related diplomatic initiatives highlight the emergence of norms related to human rights, security cooperation, and economic interaction, contributing to the gradual institutionalization of international relations (Westad, 2007). These developments suggest that even within an anarchic system, states are capable of constructing mechanisms that mitigate conflict and promote stability, albeit within certain limits.

Importantly, the Cold War should not be conceptualized as a static system. Rather, it exhibited cyclical patterns characterized by alternating phases of escalation and détente. As noted by Halliday (1983) and Westad (2007), periods of reduced tension often emerged following major crises, such as the Cuban Missile Crisis, and were subsequently followed by renewed competition. This cyclical dynamic reflects the interplay between structural constraints and agency, highlighting the importance of leadership decisions and strategic calculations in shaping international outcomes.

Table 1. Comparative Analysis of Cold War Security System and Cybersecurity Era

Dimension	Cold War Security System	Contemporary Cybersecurity System
Structure of the System	Bipolar (USA vs USSR) (Waltz, 1979)	Multipolar / Networked (state + non-state actors) (Nye, 2017)
Nature of Threats	Military, nuclear confrontation	Cyberattacks, hybrid threats, information warfare (Rid, 2013)
Key Actors	Nation-states (superpowers)	States, private sector, hacker groups, cybercriminal networks (Valeriano et al., 2018)
Domain of Conflict	Land, sea, air, nuclear	Cyberspace (fifth domain of warfare) (Kello, 2017)
Deterrence Mechanism	Nuclear deterrence (MAD)	Cyber deterrence (limited, attribution problems) (Nye, 2017)
Attribution of Attacks	Clear (state responsibility identifiable)	Difficult / ambiguous (anonymous actors) (Lindsay, 2013)
Speed of Conflict	Slow escalation	Instant / real-time attacks
Legal Framework	Developed (UN Charter, treaties)	Weak / evolving norms (Klimburg, 2017)
Role of Private Sector	Minimal	Critical (infrastructure ownership & security) (Carr, 2016)
Type of Warfare	Conventional & proxy wars	Hybrid warfare (cyber + informational + economic)

Cybersecurity as a Transformative Dimension of Contemporary Security

The transition from traditional geopolitical competition to the contemporary security environment has been profoundly influenced by the emergence of cyberspace as a critical domain of interaction. As the provided text indicates, cybersecurity introduces a set of challenges that extend beyond the capabilities of traditional state-centric security frameworks . Unlike conventional threats, cyber risks are inherently transnational, decentralized, and often difficult to attribute, thereby complicating both defensive and offensive strategies (Kello, 2017; Rid, 2013).

One of the defining characteristics of cybersecurity is the asymmetry between threat actors and state responses. Non-state actors, including hacker groups, cybercriminal organizations, and even individuals, possess the capacity to disrupt critical infrastructure and challenge state authority in unprecedented ways (Valeriano et al., 2018). This asymmetry undermines traditional assumptions regarding power distribution and raises fundamental questions about the nature of security in the digital age.

Furthermore, the increasing reliance on digital infrastructure across sectors such as energy, finance, healthcare, and transportation has amplified the potential impact of cyber threats. Attacks on critical infrastructure can have cascading effects, disrupting not only national economies but also global supply chains and communication networks (Lindsay, 2013). The case of Estonia, frequently cited in cybersecurity literature, illustrates how coordinated cyberattacks can paralyze state functions and highlight vulnerabilities within highly digitized societies (Dunn Cavelty, 2013).

The conceptualization of cyber warfare as a "second revolution in military affairs" reflects the growing recognition of cyberspace as a domain comparable to land, sea, air, and space (Singer & Friedman, 2014). However, unlike traditional domains, cyberspace lacks clearly defined boundaries, making it difficult to establish rules of engagement and determine proportional responses to attacks (Nye, 2017). This ambiguity creates significant challenges for international law and raises concerns regarding escalation and conflict management.

Table 2. Key Cybersecurity Threats, Actors, and Strategic Implications

Category	Description	Key Actors	Strategic Implications	Example
Cyber Espionage	Unauthorized access to sensitive data	State intelligence agencies, hackers	Undermines national security and diplomacy	Government database breaches
Cybercrime	Financially motivated attacks (fraud, ransomware)	Criminal networks, individuals	Economic losses, instability	Banking system attacks
Cyber Terrorism	Use of cyber tools for ideological/political goals	Terrorist groups	Fear, disruption of critical services	Infrastructure sabotage
Cyber Warfare	State-sponsored cyber operations	Nation-states, military units	Strategic advantage without kinetic war	Stuxnet attack (Lindsay, 2013)
Information Warfare	Manipulation of information and public opinion	States, media actors, bots	Political destabilization	Election interference
Critical Infrastructure Attacks	Targeting essential systems (energy, health, telecom)	State & non-state actors	Systemic collapse risk	Estonia cyberattacks (Dunn Cavelty, 2013)
Supply Chain Attacks	Exploiting vulnerabilities in software/hardware supply chains	Advanced persistent threat (APT) groups	Global systemic vulnerability	Software backdoor attacks
Hybrid Threats	Combination of cyber, economic, and political tools	States & alliances	Blurred line between war and peace	Coordinated cyber + sanctions strategy

In addition, cybersecurity challenges are compounded by governance issues, particularly in relation to the involvement of private actors. As highlighted in the original text , a substantial portion of digital infrastructure is owned and operated by private entities, necessitating new forms of public–private cooperation. Scholars argue that effective cybersecurity governance requires the integration of multiple stakeholders, including governments, corporations, and civil society organizations (Carr, 2016; Dunn Cavelty & Wenger, 2020).

The governance dimension of cybersecurity also intersects with broader concerns related to democracy and human rights. Efforts to enhance security through surveillance and data monitoring raise critical questions regarding privacy, freedom of expression, and state accountability (Buckland et al., 2015). Balancing these competing priorities represents one of the most significant challenges facing contemporary policymakers.

Emerging Strategic and Legal Dilemmas in Cybersecurity

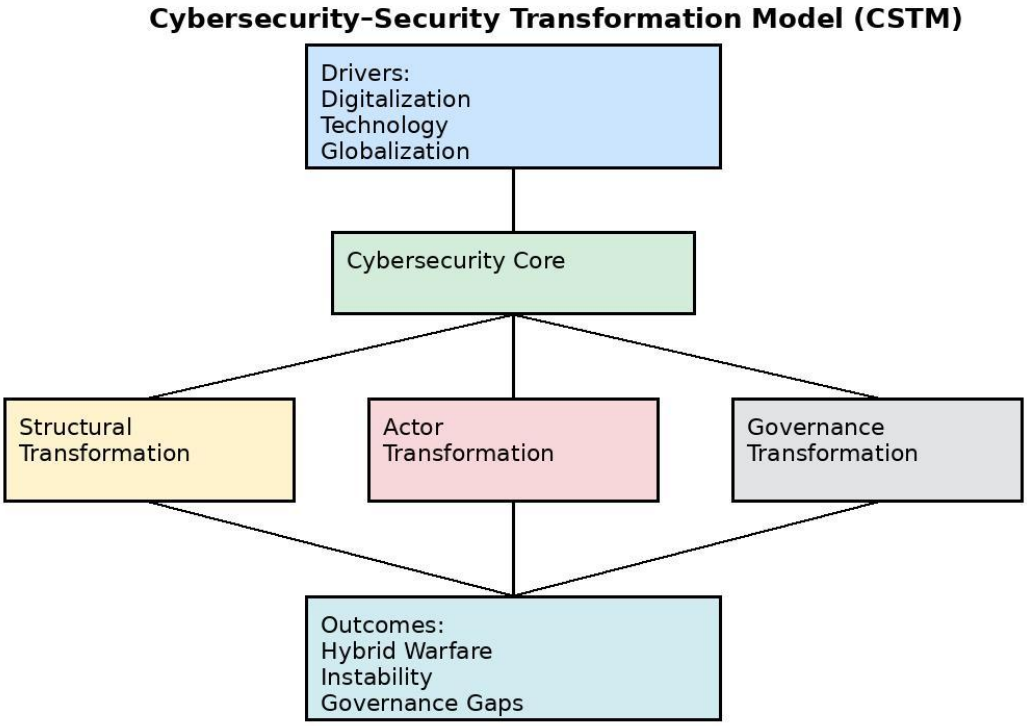
The evolution of cyber threats has introduced complex dilemmas related to attribution, proportionality, and legitimacy in international responses. One of the most persistent challenges is the difficulty of accurately identifying the perpetrators of cyberattacks. As noted in the text , actors can easily obscure their identities or impersonate others, complicating efforts to assign responsibility and implement appropriate countermeasures.

This problem of attribution has significant implications for deterrence strategies. Traditional deterrence relies on the ability to identify and punish aggressors; however, in cyberspace, the anonymity of actors undermines the credibility of retaliatory threats (Nye, 2017). As a result, states must develop alternative approaches to deterrence, including resilience-building, norm development, and international cooperation.

Moreover, the classification of cyberattacks as acts of war remains a contentious issue. The absence of universally accepted definitions of what constitutes a cyberattack, cyber espionage, or cyber warfare creates ambiguity in the application of international law (Kello, 2017). This ambiguity is further exacerbated by the dual-use nature of many cyber capabilities, which can be employed for both civilian and military purposes.

The increasing integration of cyber capabilities into national security strategies reflects a broader shift toward hybrid forms of conflict, where traditional military operations are complemented by cyber, informational, and economic tools (Valeriano et al., 2018). This hybridization of conflict blurs the boundaries between war and peace, creating a "grey zone" in which states engage in continuous competition below the threshold of armed conflict.

At the same time, international efforts to regulate cyberspace have produced a range of norms and guidelines, although their effectiveness remains limited. Initiatives led by the United Nations and regional organizations have sought to establish principles of responsible state behavior in cyberspace, including the protection of critical infrastructure and the prohibition of attacks on civilian targets (Klimburg, 2017). However, the voluntary nature of these norms and the absence of enforcement mechanisms continue to hinder their implementation.



Expanding the Analytical Framework of Cybersecurity

Given the multidimensional nature of cybersecurity, it is essential to adopt an integrated analytical framework that accounts for the interaction between technological, political, and social factors. Cybersecurity cannot be understood solely as a technical issue; rather, it represents a complex socio-political phenomenon shaped by power relations, institutional structures, and normative frameworks (Choucri, 2012).

In this regard, the concept of cyber power has emerged as a key analytical tool for understanding the role of digital capabilities in international relations. Cyber power encompasses not only the ability to conduct offensive and defensive operations but also the capacity to influence information flows, shape public opinion, and control digital infrastructure (Nye, 2017). This broader conception of power reflects the increasing importance of information and communication technologies in shaping global politics.

Furthermore, the rapid evolution of emerging technologies, including artificial intelligence and quantum computing, is likely to further transform the cybersecurity landscape. These technologies have the potential to enhance both offensive and defensive capabilities, creating new opportunities and risks for states and non-state actors alike (Kello, 2017).

Conceptual Model

This study proposes a conceptual framework, the Cybersecurity–Security Transformation Model (CSTM), to explain how cybersecurity reshapes international security systems in the digital age. The model suggests that ongoing processes such as digitalization, technological innovation, and global interconnectivity act as key drivers that elevate cybersecurity to a central domain of strategic interaction.

Within this framework, cybersecurity functions as a transformative mechanism influencing three interrelated dimensions. First, at the structural level, the international system evolves from a traditional state-centric and territorially bounded order toward a

more complex, networked, and multipolar configuration. Second, at the actor level, the dominance of states is increasingly challenged by the growing role of non-state actors, including private corporations, cyber networks, and transnational groups. Third, at the governance level, cybersecurity introduces new challenges related to regulation, accountability, and the balance between security and human rights.

Overall, the model highlights that cybersecurity is not only a technical issue but also a multidimensional geopolitical phenomenon that significantly contributes to the transformation of contemporary international security systems.

Findings

The findings of this study reveal that cybersecurity has fundamentally transformed the architecture of international security, shifting it from a predominantly state-centric and territorially bounded system to a complex, multi-actor, and transnational domain. Unlike the Cold War security paradigm, which was characterized by clearly identifiable actors and structured deterrence mechanisms, the contemporary cybersecurity environment is marked by ambiguity, asymmetry, and rapid technological evolution (Kello, 2017; Nye, 2017).

First, the analysis demonstrates that attribution remains one of the most critical challenges in cybersecurity. The inherent anonymity of cyberspace enables both state and non-state actors to conceal their identities or conduct operations through proxies, thereby complicating response strategies and undermining traditional deterrence models (Lindsay, 2013). This lack of attribution capacity weakens the effectiveness of international legal frameworks and creates an environment where accountability is difficult to enforce.

Second, the findings indicate that the role of non-state actors has significantly expanded, redefining the distribution of power within the international system. Private corporations, particularly those managing critical infrastructure and digital platforms, have become central actors in cybersecurity governance. At the same time, cybercriminal groups and hacktivist networks possess capabilities that can rival those of smaller states, thereby challenging conventional hierarchies of power (Valeriano et al., 2018; Carr, 2016).

Third, the study highlights that public–private interdependence has become a defining feature of cybersecurity governance. The majority of critical information infrastructure is owned and operated by private entities, necessitating coordinated efforts between governments and the private sector. However, this interdependence introduces governance challenges related to trust, information sharing, and accountability (Dunn Cavelty & Wenger, 2020).

Fourth, the findings emphasize that cybersecurity poses significant challenges for democratic governance and human rights. Measures aimed at enhancing cybersecurity, such as surveillance and data monitoring, often conflict with fundamental rights, including privacy and freedom of expression. This tension creates a complex policy dilemma, requiring states to balance security imperatives with the protection of civil liberties (Buckland et al., 2015).

Fifth, the analysis reveals that cyber threats increasingly target critical infrastructure, amplifying their potential impact on national and global stability. Attacks on sectors such as energy, healthcare, finance, and telecommunications can produce cascading effects, disrupting essential services and undermining public trust in institutions (Singer & Friedman, 2014).

Finally, the study finds that existing international legal and institutional frameworks remain insufficient to address the evolving nature of cyber threats. While various international agreements and guidelines have been developed, their voluntary nature and lack of enforcement mechanisms limit their effectiveness in regulating state and non-state behavior in cyberspace (Klimburg, 2017).

Conclusion

The analysis conducted in this study demonstrates that cybersecurity represents one of the most profound transformations in the evolution of international security systems. Unlike traditional security paradigms, which were largely defined by territorial boundaries, clearly identifiable actors, and structured forms of deterrence, cybersecurity introduces a multidimensional and highly dynamic environment characterized by uncertainty, complexity, and interdependence.

At the core of this transformation lies the emergence of cyberspace as a strategic domain that transcends national borders and redefines the nature of power and conflict. The ability of both state and non-state actors to operate within this domain, often anonymously and with relatively low entry barriers, has fundamentally altered the balance of power in international relations. As a result, traditional distinctions between war and peace, military and civilian targets, and domestic and international security have become increasingly blurred.

One of the central conclusions of this study is that cybersecurity creates a triple-layered challenge. First, it generates a dual security dilemma involving both public and private actors, as the protection of digital infrastructure requires coordinated efforts across multiple sectors. Second, it introduces governance challenges, particularly in democratic contexts, where the need for

effective security measures must be balanced against the protection of fundamental human rights. Third, it highlights the limitations of existing international frameworks, which struggle to keep pace with the rapid evolution of technology and the changing nature of threats.

The findings underscore the growing importance of public–private partnerships as a cornerstone of cybersecurity governance. Given that a significant portion of critical infrastructure is controlled by private entities, effective cybersecurity strategies must involve collaboration between governments, corporations, and civil society. However, this collaboration also raises important questions regarding accountability, transparency, and the distribution of responsibilities.

Furthermore, the study highlights the need to develop more robust mechanisms for attribution and response. The inability to accurately identify perpetrators of cyberattacks undermines the effectiveness of deterrence strategies and complicates efforts to enforce international norms. Addressing this challenge will require advancements in both technical capabilities and international cooperation, as well as the establishment of clearer legal standards governing state behavior in cyberspace.

Another key conclusion is that cybersecurity must be understood not only as a technical issue but also as a political and social phenomenon. The increasing use of digital technologies in governance, communication, and economic activity has created new vulnerabilities, while also providing opportunities for innovation and development. As such, cybersecurity policies must adopt a holistic approach that integrates technological solutions with broader considerations related to governance, ethics, and human rights.

In addition, the study emphasizes the importance of international norm-building and institutional development. While existing initiatives, such as United Nations guidelines and regional agreements, represent important steps toward establishing a framework for responsible behavior in cyberspace, their effectiveness remains limited by the absence of binding enforcement mechanisms. Strengthening these frameworks will be essential for ensuring stability and predictability in the international system.

Finally, the transformation of international security in the digital age calls for a re-evaluation of existing theoretical frameworks. Traditional approaches, such as realism and liberal institutionalism, provide valuable insights but are insufficient to fully capture the complexities of cyberspace. Future research should focus on developing interdisciplinary models that incorporate technological, political, and social dimensions, thereby providing a more comprehensive understanding of cybersecurity and its implications for global security.

Ethical Statement

This study was conducted in accordance with internationally accepted ethical standards in academic research. The research does not involve human participants, animals, or sensitive personal data requiring ethical approval. All sources used in the study have been properly cited in compliance with APA 7 referencing guidelines. The author confirms that the manuscript is original, has not been published elsewhere, and is not under consideration by any other journal.

The study adheres to the principles outlined by the Committee on Publication Ethics (COPE), including integrity, transparency, and responsible research conduct.

AI Usage Statement

The author declares that artificial intelligence (AI) tools were used solely for language improvement, editing, and formatting purposes. AI was not used to generate the core scientific content, analysis, or conclusions of the study. All intellectual contributions, interpretations, and academic arguments presented in this article are the sole responsibility of the author.

Acknowledgements

The author would like to express sincere gratitude to Caucasus International University for providing academic support and a research environment conducive to the completion of this study.

The author also acknowledges the contributions of scholars and researchers in the field of international security and cybersecurity whose work has significantly informed this research.

Funding

This research received no external funding. The study was conducted independently by the author without financial support from any public, commercial, or non-profit organization.

Conflict of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper. There are no financial, institutional, or personal relationships that could have influenced the research outcomes or interpretation of the findings.

References

1. Brzezinski, Z. (1992). The Cold War and its aftermath. *Foreign Affairs, 71*(4), 31–49.
2. Cohen, S. B. (2003). *Geopolitics of the world system*. Rowman & Littlefield.
3. Gaddis, J. L. (1997). *We now know: Rethinking Cold War history*. Clarendon Press.
4. Halliday, F. (1983). *The making of the Second Cold War*. Verso.
5. Kissinger, H. (2014). *World order*. Penguin Press.
6. Neocleous, M. (2006). From social to national security: On the fabrication of economic order. *Security Dialogue, 37*(3), 363–384.
7. Hasib, M. (2015). *Cybersecurity leadership: Powering the modern organization*. Springer.
8. Howard, R. (2023). *Cybersecurity first principles: A reboot of strategy and tactics*. CRC Press.
9. Buckland, B. S., Schreier, F., & Winkler, T. H. (2015). *Democratic governance challenges of cybersecurity*. Geneva Centre for the Democratic Control of Armed Forces. https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf
10. Svanadze, V. (2015). *Cyberspace and cybersecurity challenges*. Tbilisi.
11. Svanadze, V., & Gotsiridze, A. (2015). *Key actors in cyberspace, cybersecurity policy, strategy and challenges*. Tbilisi.
12. Maisaia, V., & Guchua, A. (2020). *NATO and non-state actors*. Tbilisi.
13. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Computers & Security, 83*, 336–352. https://doi.org/10.1016/j.cose.2019.02.016
14. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504
15. Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.
16. Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*(1), 105–122.
17. Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32.
18. Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
19. Klimburg, A. (Ed.). (2017). *National cyber security framework manual*. NATO CCDCOE Publication.
20. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
21. Najafov, R. (2025). Socio-psychological factors of youth deviant behavior in the contemporary era and their impact on social development mechanisms: Forms and patterns of influence. *ECOSOCIAL Studies: Banking, Finance and Cybersecurity, 7*(2), 13–28. https://doi.org/10.56334/ecosbankfincyber/7.2.3
22. Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.
23. Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
24. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
25. Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.