Multidisciplinary Bulletin of Global Scholarship
ISSN (Online): XXXX-XXXX
Received: 02-01-2026, Revised: 11-01-2026
Accepted: 12-02-2026, Published: 08-08-2026
DOI: https://doi.org/10.69526/mbgs.v1i1.453

Artificial Intelligence, Cyber Power, And National Security: Redefining State Sovereignty In The Twenty-First Century

Francis C. Okpo[1]; Mukhtar Imam[2]; Joseph O. Odama[3];

Abstract

Purpose – *The rapid advancement of Artificial Intelligence (AI) and cyberspace technologies has fundamentally transformed the global security environment, challenging conventional understandings of sovereignty, military power, governance, and interstate relations. This study examines the intersection between AI, cyber power, and national security, with the aim of explaining how AI is redefining state sovereignty within an increasingly interconnected digital ecosystem.* **Design/methodology/approach** – *This study employs a qualitative research design based on documentary analysis, comparative policy evaluation, and theoretical synthesis. It integrates perspectives from Realism, Liberal Institutionalism, Constructivism, and Cyber Sovereignty Theory to examine the strategic implications of AI-driven cyber capabilities. The analysis draws on contemporary policy documents, academic literature, and international reports concerning cyber governance, AI development, and national security.* **Findings** – *The findings demonstrate that AI has emerged as a force multiplier that is reshaping military doctrine, intelligence operations, cyber deterrence, digital governance, and geopolitical competition. AI-powered cyber capabilities enhance intelligence gathering, critical infrastructure protection, and military modernization, while simultaneously introducing unprecedented security risks, including autonomous cyber weapons, algorithmic manipulation, misinformation campaigns, deepfakes, cyber espionage, and sophisticated attacks on critical infrastructure. The analysis further suggests that future state sovereignty will depend increasingly on digital resilience, technological innovation, cyber defense capacity, and effective AI governance rather than solely on territorial control or conventional military strength.* **Research implications/limitations** – *This study is conceptual in nature and relies on documentary sources and comparative policy analysis. Future research should incorporate empirical case studies and quantitative assessments of AI-enabled cyber operations to evaluate their effectiveness, risks, and implications across different national contexts.* **Originality/value** – *This study contributes to contemporary security studies by integrating major international relations theories with Cyber Sovereignty Theory to explain the transformation of national security in the AI era. It proposes a comprehensive analytical framework demonstrating that sustainable sovereignty in the twenty-first century increasingly depends on the integration of AI governance, cyber resilience, indigenous technological innovation, and multilateral cooperation for responsible AI deployment.*

Keywords: *Artificial Intelligence; Cyber Power; National Security; State Sovereignty; Cyber Warfare; AI Governance; Digital Sovereignty; International Security; Cyber Deterrence; Strategic Competition.*

[1] National Institute for Security Studies, Lower Usuma Dam, Abuja-Nigeria.
Email: nwaigwenezuruoha@gmail.com
[2] Almuhibbah Open University, Abuja, Nigeria, Corresponding Email: mukhtarimam01@gmail.com
[3] National Institute for Security Studies, Lower Usuma Dam, Abuja-Nigeria.
Email: Joeodema2017@gmail.com

Introduction

The emergence of Artificial Intelligence (AI) represents one of the most transformative technological revolutions since the Industrial Revolution. Over the past decade, AI has transitioned from a specialized computational discipline into a strategic asset influencing virtually every aspect of governance, economics, military affairs, and international politics (Russell & Norvig, 2021). Governments increasingly perceive AI not merely as a technological innovation but as a determinant of national competitiveness, geopolitical influence, and strategic autonomy (Kissinger et al., 2021). Simultaneously, cyberspace has evolved into the fifth operational domain of warfare alongside land, sea, air, and space, fundamentally reshaping the conduct of conflict and statecraft (Nye, 2017).

Traditional understandings of national security were largely premised upon territorial integrity, military strength, and political sovereignty. Classical theorists such as Hobbes (1651), Machiavelli (1532), and Morgenthau (1948) conceptualized sovereignty primarily through the state's monopoly over legitimate violence and its capacity to defend territorial boundaries. However, globalization and digital interconnectedness have increasingly eroded the exclusivity of territorial sovereignty. Contemporary threats frequently originate beyond national borders and propagate through interconnected digital networks, making physical borders less effective as security barriers (Singer & Friedman, 2014).

Artificial Intelligence amplifies this transformation by introducing autonomous decision-making systems capable of processing enormous volumes of information at unprecedented speed. AI-driven technologies support intelligence analysis, predictive policing, cybersecurity, autonomous weapons systems, surveillance, logistics, financial monitoring, border control, and strategic military planning. Consequently, AI is becoming central to both offensive and defensive dimensions of national security.

Cyber power similarly represents a departure from traditional military capabilities. Joseph Nye (2017) defines cyber power as the ability to achieve desired outcomes through the use of electronically connected information resources. Unlike conventional military force, cyber power allows states to disrupt financial systems, manipulate elections, compromise critical infrastructure, conduct espionage, steal intellectual property, and influence public opinion without crossing physical borders.

The convergence of AI and cyber capabilities has generated an entirely new security paradigm. AI-powered cyber attacks increasingly exploit machine learning algorithms to identify software vulnerabilities, automate phishing campaigns, bypass security protocols, generate sophisticated malware, and

evade traditional cybersecurity mechanisms (Brundage et al., 2018). Conversely, AI also enhances defensive capabilities by enabling real-time anomaly detection, predictive threat intelligence, automated incident response, and adaptive cyber defense systems.

The implications extend beyond technical considerations. AI challenges fundamental assumptions regarding sovereignty, accountability, legal responsibility, and strategic stability. Autonomous cyber weapons capable of initiating attacks without direct human intervention raise profound ethical and legal questions concerning the laws of armed conflict, proportionality, and state responsibility (Scharre, 2018). Moreover, AI-driven misinformation campaigns and deepfake technologies undermine democratic institutions by manipulating public opinion and eroding trust in information ecosystems.

Major powers have therefore integrated AI into broader national security strategies. The United States regards AI as a cornerstone of military modernization and strategic competition (U.S. Department of Defense, 2023). China has declared its ambition to become the global leader in AI by 2030 while emphasizing cyber sovereignty and technological self-reliance (State Council of China, 2017). Russia similarly views AI as a strategic equalizer capable of offsetting conventional military asymmetries (President of Russia, 2019). These developments indicate that AI has become a critical dimension of geopolitical competition.

Developing countries equally face significant implications. African states increasingly depend upon digital infrastructure for governance, banking, healthcare, elections, and economic development. Yet many remain vulnerable to cybercrime, digital espionage, infrastructure attacks, and foreign technological dependence due to limited cybersecurity capacity, inadequate legal frameworks, and shortages of skilled professionals (African Union, 2024). Consequently, the digital divide increasingly constitutes a national security concern.

This article argues that Artificial Intelligence and cyber power are fundamentally redefining state sovereignty by shifting strategic competition from physical territory toward control of digital infrastructure, information ecosystems, technological innovation, and cyber resilience. The paper examines the evolving relationship between AI, cyber power, and national security while proposing policy measures for strengthening digital sovereignty in the twenty-first century.

Background of the Study

The concept of sovereignty has undergone continuous transformation throughout international history. Following the Peace of Westphalia in 1648, sovereignty became associated with territorial integrity, political independence, and non-interference in domestic affairs. The Westphalian model established the state as the supreme authority within clearly defined geographical boundaries (Krasner, 1999). For centuries, military capability determined sovereignty. Powerful armies, naval superiority, industrial capacity, and later nuclear deterrence constituted the principal instruments through which states protected national interests. During the Cold War, geopolitical competition largely revolved around ideological rivalry, nuclear deterrence, conventional military alliances, and proxy conflicts (Waltz, 1979).

The information revolution fundamentally altered this paradigm. Beginning in the late twentieth century, the widespread diffusion of computers, the Internet, satellite communications, and digital technologies transformed economic production, governance, intelligence, and military operations. Information itself became a strategic resource comparable to oil, industrial production, and military hardware. Cybersecurity consequently emerged as an integral component of national security. High-profile incidents—including the 2007 cyber attacks on Estonia, the Stuxnet operation against Iran's nuclear facilities in 2010, the 2015 cyber attack on Ukraine's power grid, the SolarWinds breach, and subsequent ransomware campaigns—demonstrated the capacity of cyber operations to inflict strategic damage without conventional military engagement.

Artificial Intelligence accelerated this transformation by introducing unprecedented automation into cyberspace. Machine learning algorithms continuously monitor global networks, identify anomalies, detect malicious behavior, optimize resource allocation, and support intelligence analysis. Offensive cyber capabilities likewise increasingly employ AI to automate reconnaissance, vulnerability assessment, malware adaptation, credential theft, and social engineering attacks. The convergence of AI and cyber operations has profound implications for military affairs. Autonomous drones, intelligent surveillance systems, predictive logistics, battlefield decision support, and AI-assisted command-and-control systems are redefining military doctrine. The integration of AI into defense planning enables faster decision cycles while introducing concerns about reliability, bias, escalation risks, and human oversight.

Beyond warfare, AI influences economic security, public health, border management, energy systems, transportation networks, financial services, and

democratic governance. Critical infrastructure increasingly relies upon interconnected digital systems that simultaneously enhance efficiency and create vulnerabilities exploitable through cyber attacks.

Digital platforms also shape political communication. AI-powered recommendation systems, automated content generation, deepfake technology, and algorithmic amplification influence electoral processes, public discourse, and societal trust. Consequently, national security increasingly encompasses information integrity, digital resilience, and technological governance. International institutions have begun responding to these developments through emerging frameworks addressing responsible AI use, cyber norms, confidence-building measures, and digital governance. Nevertheless, consensus remains elusive because major powers possess divergent strategic interests concerning data governance, cyber sovereignty, cross-border information flows, and technological competition.

As AI capabilities continue advancing, sovereignty itself increasingly depends upon technological independence, cybersecurity capacity, indigenous innovation, digital infrastructure resilience, and strategic control over critical technologies.

Statement of the Problem

The rapid convergence of Artificial Intelligence and cyber technologies has fundamentally transformed the nature of national security threats while exposing significant inadequacies in existing governance structures, international legal frameworks, and strategic doctrines. Traditional conceptions of sovereignty remain largely anchored in territorial control despite contemporary threats originating primarily through borderless digital networks.

AI-enabled cyber operations increasingly challenge states' ability to safeguard critical infrastructure, democratic institutions, economic systems, and military assets. Autonomous cyber attacks, algorithmic misinformation, deepfake technologies, and AI-assisted espionage complicate attribution, weaken deterrence, and create uncertainty regarding legal responsibility. Furthermore, technological asymmetries have intensified geopolitical competition. Major powers dominate AI research, semiconductor production, cloud infrastructure, quantum computing, and cybersecurity innovation, while developing countries remain technologically dependent upon foreign digital ecosystems. This dependence creates strategic vulnerabilities affecting political autonomy, economic development, and national resilience.

Existing international law provides limited guidance regarding autonomous cyber weapons, AI-enabled conflict, digital sovereignty, and cross-

border cyber operations. The absence of universally accepted norms increases the risk of escalation, miscalculation, and strategic instability. For many developing countries, including those in Africa, limited institutional capacity, inadequate cybersecurity legislation, shortages of AI expertise, and dependence on imported technologies further undermine digital sovereignty. Consequently, there is an urgent need to understand how AI and cyber power redefine sovereignty and national security within the evolving international system.

Method

This study adopts a qualitative research design employing doctrinal analysis, comparative case studies, documentary analysis, and theoretical synthesis. Secondary data were collected from peer-reviewed journal articles, government policy documents, international organization reports, defense strategies, cybersecurity frameworks, and reputable think tanks. The study utilizes purposive sampling to examine prominent AI powers including the United States, China, Russia, the European Union, Israel, and Nigeria as representative cases illustrating different approaches to AI governance, cyber capability development, and national security. Data are analyzed using thematic content analysis, allowing patterns relating to cyber power, AI governance, military modernization, sovereignty, and strategic competition to emerge. Comparative analysis facilitates cross-national evaluation of AI strategies and cyber policies.

Theoretical Framework

Understanding the relationship between Artificial Intelligence (AI), cyber power, and national security requires an interdisciplinary theoretical approach. No single international relations theory adequately explains the technological transformation currently reshaping global politics. Consequently, this study adopts a multi-theoretical framework combining Classical Realism, Neorealism, Liberal Institutionalism, Constructivism, Cyber Sovereignty Theory, and Technological Determinism. Together, these perspectives provide complementary explanations of how AI influences state behavior, power competition, security policy, and sovereignty.

Classical Realism

Realism remains one of the most influential theories in international relations for explaining national security and interstate competition. Rooted in the works of Thucydides, Machiavelli, Hobbes, Carr (1939), and Morgenthau (1948), realism assumes that the international system is anarchic, with no central authority capable of guaranteeing state security. States therefore prioritize survival, accumulate power, and pursue national interests through military,

economic, diplomatic, and technological capabilities. Artificial Intelligence fits naturally within realist assumptions because technological superiority has historically translated into military and geopolitical advantage. AI has become an emerging strategic resource comparable to nuclear technology during the Cold War. States increasingly invest in AI because they recognize that technological leadership determines future military superiority, intelligence capabilities, and economic competitiveness (Horowitz, 2018).

The United States, China, and Russia exemplify realist behavior through extensive investments in AI-driven defense systems, autonomous weapons, cyber intelligence, quantum computing, and advanced surveillance. Their competition illustrates the contemporary security dilemma, whereby one state's technological advancement is perceived as another state's security threat, prompting reciprocal investments and accelerating an AI arms race (Jervis, 1978). From a realist perspective, cyber power constitutes another instrument through which states maximize relative power. Offensive cyber capabilities enable intelligence collection, strategic disruption, economic coercion, and military advantage while avoiding conventional warfare. AI further enhances these capabilities by automating cyber operations, improving predictive intelligence, and accelerating decision-making. However, realism alone inadequately explains growing international cooperation in cybersecurity, digital governance, and AI ethics. Therefore, complementary theoretical perspectives are necessary.

Neorealism (Structural Realism)

Kenneth Waltz (1979) refined realism by arguing that international outcomes are primarily determined by the structure of the international system rather than individual state characteristics. Under anarchy, states continuously seek security through balancing behavior. Neorealism helps explain contemporary AI competition. Technological capabilities increasingly determine the distribution of global power. States possessing advanced semiconductor industries, AI research institutions, quantum computing infrastructure, and cyber capabilities enjoy structural advantages over technologically dependent nations. The current strategic rivalry between the United States and China illustrates structural realism. Both countries perceive AI leadership as essential to maintaining or attaining systemic dominance. Their investments in AI research, semiconductor manufacturing, cloud infrastructure, satellite systems, and cybersecurity represent balancing strategies within an evolving multipolar international order.

Similarly, Russia's emphasis on AI-enabled military modernization seeks to offset conventional economic limitations by leveraging technological innovation as an asymmetric strategic equalizer.

Neorealism also explains why developing countries increasingly view digital dependence as a national security concern. Reliance on foreign cloud providers, software ecosystems, communication infrastructure, and AI platforms potentially limits strategic autonomy and weakens sovereignty.

Liberal Institutionalism

Unlike realism, Liberal Institutionalism argues that international cooperation is both possible and necessary despite anarchy. Scholars including Keohane (1984) and Nye (2004) emphasize the role of institutions, norms, interdependence, and international organizations in reducing conflict. Artificial Intelligence presents numerous challenges requiring collective governance. Cyber threats frequently transcend national borders, affecting financial systems, healthcare infrastructure, aviation, telecommunications, and global supply chains. Consequently, unilateral security strategies prove insufficient.

International organizations increasingly facilitate cooperation on AI governance. Examples include:

- United Nations discussions on autonomous weapons
- OECD AI Principles
- UNESCO Recommendation on the Ethics of Artificial Intelligence
- Global Partnership on AI (GPAI)
- European Union AI Act
- NATO AI Strategy
- African Union Continental AI Strategy

These initiatives illustrate liberal institutionalism's argument that international rules and norms reduce uncertainty while promoting responsible technological development. However, institutional cooperation remains constrained by geopolitical competition. Major powers frequently disagree regarding data governance, digital sovereignty, internet regulation, and AI standards.

Constructivism

Constructivism argues that international politics is socially constructed through ideas, identities, norms, and shared understandings rather than solely material capabilities (Wendt, 1999). This perspective is particularly relevant because AI influences not only military power but also societal perceptions, political legitimacy, and information environments. Cyber operations increasingly target narratives rather than infrastructure alone. AI-generated misinformation, deepfakes, automated propaganda, and algorithmic manipulation reshape political discourse and public opinion. Constructivists argue that sovereignty itself is evolving because social understandings of

authority have changed. Whereas sovereignty once emphasized territorial borders, contemporary interpretations increasingly include:

- Digital sovereignty
- Data sovereignty
- Information sovereignty
- Technological sovereignty

States now seek control over data flows, AI development, digital platforms, and communication infrastructure alongside traditional territorial governance. Constructivism therefore explains why concepts such as "digital independence" and "technological self-reliance" have become central political narratives in countries including China, India, Russia, and members of the European Union.

Cyber Sovereignty Theory

Cyber Sovereignty Theory represents one of the most influential contemporary perspectives on digital governance. The theory argues that states possess sovereign authority over cyberspace within their jurisdictions just as they possess authority over physical territory (Mueller, 2010). China has emerged as the leading advocate of cyber sovereignty, emphasizing governmental control over domestic internet infrastructure, data governance, artificial intelligence regulation, and cross-border information flows. Under this framework, sovereignty extends beyond physical borders to include:

- National data
- Digital infrastructure
- Cloud services
- Internet governance
- Artificial Intelligence
- Critical information infrastructure

Cyber sovereignty challenges the earlier liberal vision of an open, borderless internet. Instead, governments increasingly regulate digital platforms according to domestic political, economic, and security priorities. The theory is particularly relevant because AI systems depend heavily upon data collection, cloud computing, algorithmic control, and digital infrastructure—all areas increasingly viewed as strategic national assets.

Technological Determinism

Technological Determinism argues that technological innovation fundamentally transforms societies, political systems, institutions, and economic structures (McLuhan, 1964). AI exemplifies this phenomenon. Machine learning, robotics, autonomous systems, natural language processing, and predictive analytics have fundamentally altered:

- intelligence collection
- military logistics
- surveillance
- public administration
- healthcare
- transportation
- financial security
- law enforcement

Technological advances often outpace legal and institutional adaptation. Consequently, governments continually revise national security doctrines to accommodate emerging technological realities. Technological Determinism therefore explains why AI increasingly drives policy rather than merely supporting existing policy.

Integrated Theoretical Model

This study synthesizes these theories into an integrated analytical framework.

Table 1. *Theoretical Contributions to the Analysis of AI, Global Competition, and Digital Sovereignty*

Theory	**Contribution to Study**
Classical Realism	AI as strategic power
Neorealism	Global AI competition
Liberal Institutionalism	International AI governance
Constructivism	Evolution of sovereignty
Cyber Sovereignty Theory	Digital territorial control
Technological Determinism	Technology-driven political transformation

Source: *Author's synthesis*

Collectively, these theories demonstrate that AI transforms both the material and ideational foundations of national security.

Conceptualizing Artificial Intelligence

Artificial Intelligence has evolved considerably since John McCarthy coined the term in 1956. Contemporary AI encompasses machine learning, deep learning, computer vision, natural language processing, reinforcement learning, and generative AI. Russell and Norvig (2021) define AI as the study of intelligent agents capable of perceiving environments and acting autonomously to achieve specified objectives. Kaplan and Haenlein (2019) emphasize AI's ability to imitate human cognitive functions including learning, reasoning, problem solving, perception, and language understanding. Recent advances in generative AI have dramatically expanded AI capabilities beyond prediction toward content generation, autonomous coding, strategic planning, and scientific discovery. Governments increasingly regard AI as general-purpose technology comparable to electricity or the internet because it transforms virtually every economic sector.

Evolution of Cyber Power

Joseph Nye (2010; 2017) introduced cyber power as the ability to obtain preferred outcomes through electronically connected information resources. Cyber power differs fundamentally from conventional military power.

Traditional power relies upon:

- territorial occupation
- military force
- industrial capacity

Cyber power relies upon:

- information superiority
- digital infrastructure
- software
- data
- connectivity
- computational capability

Libicki (2009) argues that cyberspace has become a distinct operational domain where strategic competition occurs continuously below the threshold of conventional warfare.

Cyber operations include:

- espionage
- sabotage
- ransomware
- influence campaigns

- election interference
- infrastructure disruption

Unlike traditional warfare, cyber conflict often lacks clear attribution, enabling plausible deniability.

Artificial Intelligence as National Power

Power has historically evolved through successive technological revolutions.

Agricultural Revolution → Land

Industrial Revolution → Manufacturing

Nuclear Revolution → Atomic capability

Information Revolution → Information

AI Revolution → Intelligence

Horowitz (2018) argues that AI represents the next military revolution because intelligent systems improve battlefield awareness, logistics, targeting, and operational speed.

AI influences nearly every dimension of national power including:

- Economic productivity
- Military modernization
- Scientific research
- Industrial competitiveness
- Diplomatic influence
- Cybersecurity
- Space technology
- Intelligence operations

Consequently, governments increasingly classify AI as critical national infrastructure.

AI and Military Transformation

Military institutions worldwide increasingly integrate AI across operational domains.

Applications include:

- Autonomous drones
- Decision support systems
- Predictive maintenance
- Satellite image analysis
- Target recognition
- Swarm robotics
- Cyber defense
- Electronic warfare
- Intelligence fusion

The U.S. Department of Defense's Joint All-Domain Command and Control (JADC2) initiative exemplifies AI-enabled military integration. Similarly, China's People's Liberation Army pursues "intelligentized warfare," integrating AI across command systems, logistics, unmanned platforms, and strategic planning. Russia likewise invests heavily in AI-supported electronic warfare and autonomous combat systems. These developments collectively constitute the Fourth Military Revolution.

Artificial Intelligence and Intelligence Collection

Intelligence agencies increasingly depend upon AI because modern surveillance generates enormous quantities of data.

Machine learning enables:

- facial recognition
- voice identification
- pattern recognition
- financial intelligence
- social media monitoring
- behavior prediction
- satellite imagery interpretation
- cyber threat detection

Open-source intelligence (OSINT) has become increasingly valuable due to AI's ability to synthesize publicly available information rapidly. However,

scholars warn that AI-generated intelligence may reinforce algorithmic bias if training datasets are incomplete or politically skewed.

Artificial Intelligence and Cybersecurity

Cybersecurity has become one of AI's most important applications.

Traditional security relied upon:

- signature-based detection
- manual monitoring
- rule-based systems
- AI introduces:
- behavioral analytics
- adaptive defense
- predictive threat intelligence
- anomaly detection
- automated incident response
- zero-day vulnerability prediction

Darktrace, Microsoft Defender, Google's Chronicle, CrowdStrike Falcon, and SentinelOne illustrate commercial AI-powered cybersecurity platforms that continuously learn from network behavior. AI reduces response times from hours to seconds. Nevertheless, attackers similarly employ AI to automate phishing campaigns, malware generation, password cracking, reconnaissance, and vulnerability discovery. Consequently, cybersecurity increasingly represents an AI-versus-AI competition.

AI-Driven Cyber Warfare

Cyber warfare has evolved beyond isolated hacking incidents. Modern campaigns increasingly integrate:

- Artificial Intelligence
- Big Data
- Cloud Computing
- Internet of Things
- Satellite Systems
- Machine Learning
- Quantum Computing
- Autonomous Systems
- AI enables offensive cyber operations through:
- automated malware evolution

- network reconnaissance
- credential harvesting
- deepfake generation
- disinformation
- social engineering
- adversarial machine learning

These developments reduce operational costs while increasing attack sophistication. Researchers increasingly describe future cyber conflict as "algorithmic warfare."

Sovereignty in the Digital Age

The classical Westphalian conception of sovereignty emphasized territorial integrity.

- Digital globalization challenges this assumption.
- Information now crosses borders instantaneously.
- Cloud services distribute data globally.
- Digital platforms influence domestic politics.
- Artificial Intelligence processes transnational datasets.

Consequently, scholars increasingly distinguish between:

- Political sovereignty
- Economic sovereignty
- Data sovereignty
- Digital sovereignty
- Technological sovereignty
- Algorithmic sovereignty
- States increasingly seek domestic control over:
- AI models
- Cloud infrastructure
- Semiconductor manufacturing
- Critical data
- Telecommunications
- Cybersecurity infrastructure
- Digital payment systems

The literature increasingly recognizes that sovereignty extends beyond geography into digital ecosystems.

Literature Gap

Despite rapid growth in AI scholarship, several important gaps remain.

First, many studies examine Artificial Intelligence primarily from technological or engineering perspectives while neglecting broader implications for international relations and sovereignty. Second, cybersecurity literature often focuses on technical defense mechanisms rather than the geopolitical consequences of AI-enabled cyber power.

Third, studies addressing sovereignty frequently rely upon traditional territorial frameworks that inadequately capture emerging forms of digital authority, algorithmic governance, and technological dependence. Fourth, relatively few comparative analyses examine how both major powers and developing countries—including African states—are responding to AI-driven transformations in national security. Finally, existing research tends to analyze AI, cyber power, and national security as separate domains rather than as interconnected elements reshaping the contemporary international system. Accordingly, this study contributes to the literature by developing an integrated analytical framework that explains how Artificial Intelligence and cyber power collectively redefine state sovereignty, alter strategic competition, and reshape national security in the twenty-first century.

Artificial Intelligence as a Strategic Instrument of State Power

Artificial Intelligence (AI) has rapidly evolved from a specialized computational technology into one of the defining instruments of state power in the twenty-first century. Historically, geopolitical influence was measured through territory, military strength, industrial capacity, and economic resources. However, the digital revolution has introduced a new hierarchy of power in which computational capability, algorithmic superiority, data governance, and technological innovation increasingly determine national competitiveness (Kissinger, Schmidt, & Huttenlocher, 2021). Consequently, AI is no longer viewed merely as an economic driver but as a strategic national asset capable of shaping military superiority, diplomatic leverage, intelligence operations, and economic resilience.

The concept of national power has traditionally been understood through comprehensive frameworks such as DIME (Diplomatic, Information, Military, and Economic power). Artificial Intelligence now permeates each of these dimensions. Diplomatically, AI enhances predictive foreign policy analysis and strategic communication. Informationally, AI enables rapid data processing, disinformation detection, and narrative influence. Militarily, AI transforms command-and-control systems, autonomous weapons, logistics, surveillance,

and battlefield decision-making. Economically, AI drives innovation, productivity, and technological competitiveness (Horowitz, 2018).

The strategic significance of AI stems primarily from its ability to convert data into actionable intelligence at unprecedented speed. Governments generate enormous volumes of data through satellites, intelligence services, financial systems, border controls, telecommunications, and social media. Machine learning algorithms synthesize these datasets into predictive insights that support strategic planning, risk assessment, and operational decision-making (Russell & Norvig, 2021). Unlike conventional computational systems that rely on predefined instructions, AI continuously learns and adapts to evolving environments, thereby increasing its strategic utility across diverse policy domains.

One of the most significant implications of AI for state power is the acceleration of decision-making cycles. Boyd's (1987) Observe–Orient–Decide–Act (OODA) Loop remains influential in military strategy, emphasizing that actors capable of making decisions faster than adversaries gain substantial strategic advantages. AI compresses each stage of the OODA Loop by automating data collection, environmental analysis, threat prioritization, and response recommendations. States possessing superior AI capabilities therefore acquire strategic advantages not only through enhanced military capacity but also through superior situational awareness and adaptive decision-making.

Moreover, AI strengthens economic statecraft by supporting industrial automation, supply chain optimization, financial forecasting, and scientific research. Countries leading AI innovation increasingly dominate emerging technologies including robotics, semiconductor manufacturing, quantum computing, biotechnology, and advanced materials. Consequently, technological leadership increasingly determines geopolitical influence. As Nye (2024) observes, the future balance of power will depend less on the size of conventional armed forces than on the capacity to innovate and control strategic technologies.

Artificial Intelligence and the Transformation of Cyber Power

Cyberspace has emerged as the fifth operational domain of warfare alongside land, sea, air, and space. Within this domain, AI fundamentally transforms both offensive and defensive cyber capabilities. Cyber power is no longer measured solely by the number of skilled hackers or offensive cyber tools but increasingly by the ability to integrate AI into cyber operations (Nye, 2017).

Artificial Intelligence enhances cyber power in four principal ways: automation, prediction, adaptation, and scalability. Automation enables AI systems to perform tasks that previously required extensive human intervention.

These include vulnerability scanning, malware analysis, intrusion detection, incident response, and network monitoring. Automated cyber defense significantly reduces response times while increasing operational efficiency. Prediction constitutes another transformative capability. AI systems analyze historical attack patterns, network behavior, and threat intelligence to anticipate future cyber incidents. Predictive analytics enable governments to strengthen vulnerable infrastructure before attacks occur rather than reacting after damage has been sustained (Brundage et al., 2018).

Adaptation distinguishes AI from traditional software. Conventional cybersecurity relies primarily on static rules and known attack signatures. AI systems continuously learn from emerging threats, modifying defensive strategies in real time. This adaptive capacity is particularly valuable against sophisticated Advanced Persistent Threats (APTs) that evolve continuously. Scalability further amplifies cyber power. Machine learning systems simultaneously monitor millions of digital interactions across government agencies, financial institutions, energy systems, healthcare networks, transportation infrastructure, and military communications. Human analysts cannot process comparable volumes of information without AI assistance. However, these advantages equally benefit malicious actors. Cybercriminal organizations increasingly employ AI to automate phishing attacks, identify software vulnerabilities, generate polymorphic malware, bypass security controls, and conduct large-scale credential theft. This creates an "AI versus AI" cybersecurity environment in which both attackers and defenders continuously improve algorithmic capabilities. The democratization of AI also complicates strategic stability. Advanced cyber capabilities once required substantial governmental resources. Today, commercially available AI tools enable relatively small organizations to conduct sophisticated cyber operations, thereby reducing barriers to offensive cyber activity. Consequently, cyber power is no longer monopolized by technologically advanced states but increasingly diffused among non-state actors.

Artificial Intelligence and National Security

National security has traditionally focused on protecting territorial integrity, political independence, and military sovereignty. Contemporary security, however, increasingly encompasses economic resilience, technological innovation, digital infrastructure, public health, information integrity, and societal stability (Buzan, Wæver, & de Wilde, 1998). AI influences each of these dimensions simultaneously.

First, AI enhances intelligence capabilities through advanced data analytics. Intelligence agencies process enormous quantities of satellite imagery,

intercepted communications, financial transactions, social media activity, and open-source intelligence. Machine learning algorithms rapidly identify patterns, anomalies, and emerging threats that human analysts might overlook. Second, AI strengthens border security. Intelligent surveillance systems combine facial recognition, biometric verification, behavioral analytics, and autonomous monitoring to improve immigration control, customs enforcement, and counterterrorism operations. These systems increase operational efficiency while reducing dependence on manual inspection.

Third, AI improves emergency response and crisis management. Governments increasingly employ predictive analytics to forecast natural disasters, disease outbreaks, cyber incidents, and infrastructure failures. Early warning systems enhance preparedness while minimizing economic and human losses. Fourth, AI contributes significantly to economic security. Financial institutions increasingly depend upon AI to detect fraud, monitor systemic risks, optimize investment strategies, and safeguard digital payment systems. Since economic stability constitutes an essential component of national security, AI indirectly strengthens overall state resilience. Fifth, AI enhances counterterrorism capabilities. Machine learning algorithms analyze communication networks, financial transactions, travel records, and behavioral indicators to identify potential terrorist activities before attacks occur. Nevertheless, scholars caution that predictive policing and algorithmic surveillance may produce discriminatory outcomes if datasets contain embedded social biases (O'Neil, 2016). National security agencies therefore face a dual challenge: maximizing AI's strategic benefits while mitigating ethical, legal, and societal risks associated with algorithmic governance.

Artificial Intelligence, Military Modernization, and the Future Battlefield

Military institutions worldwide increasingly regard Artificial Intelligence as the defining technology of future warfare. Previous military revolutions centered upon gunpowder, mechanization, nuclear weapons, and information technology. AI now represents the foundation of what many analysts describe as the Fifth Military Revolution (Scharre, 2018).

AI transforms military capability across every operational domain.

Land Operations

Ground forces increasingly employ autonomous reconnaissance vehicles, robotic logistics platforms, intelligent surveillance systems, and AI-assisted command networks. Autonomous ground vehicles reduce personnel exposure while improving operational effectiveness in contested environments.

Air Operations

Military aviation increasingly integrates AI into mission planning, predictive maintenance, target recognition, autonomous navigation, and drone swarms. AI-assisted combat aircraft process sensor information significantly faster than human pilots, enhancing battlefield awareness.

Maritime Operations

Naval forces employ autonomous underwater vehicles, intelligent sonar systems, maritime surveillance platforms, and AI-supported fleet logistics. These technologies improve anti-submarine warfare, mine detection, and maritime domain awareness.

Space Operations

Artificial Intelligence increasingly supports satellite navigation, orbital surveillance, missile warning systems, debris monitoring, and space traffic management. As space becomes increasingly contested, AI enhances resilience against anti-satellite operations.

Cyber Operations

Cyber commands integrate AI into malware detection, vulnerability assessment, network defense, intelligence collection, and offensive cyber operations. AI enables cyber forces to identify adversarial activities in near real time. One of the most controversial aspects of military AI concerns autonomous weapons systems. These systems possess varying degrees of independence in selecting and engaging targets. Advocates argue that autonomous systems improve precision while reducing military casualties. Critics contend that delegating lethal decision-making to machines raises profound ethical, legal, and humanitarian concerns. The United Nations Convention on Certain Conventional Weapons (CCW) continues to debate international regulation of Lethal Autonomous Weapons Systems (LAWS). Nevertheless, technological development substantially outpaces diplomatic negotiations, increasing concerns regarding an uncontrolled AI arms race.

AI-Enabled Cyber Warfare and Hybrid Threats

Artificial Intelligence has fundamentally transformed cyber warfare by increasing operational speed, sophistication, precision, and scalability. Traditional cyber attacks typically required extensive human planning and manual execution. AI now automates significant portions of offensive cyber operations, enabling attackers to identify vulnerabilities, generate malicious code, and adapt attack strategies with minimal human intervention (Brundage et al., 2018).

Machine learning algorithms facilitate automated reconnaissance by continuously scanning digital networks for exposed services, software weaknesses, and misconfigured systems. Once vulnerabilities are identified, AI-powered tools prioritize targets according to strategic value and likelihood of successful exploitation. Generative AI further accelerates offensive operations by assisting in malware development, phishing content creation, and social engineering campaigns. AI has also enhanced ransomware operations. Criminal organizations increasingly employ AI to identify high-value victims, optimize encryption strategies, and automate negotiations. These developments have contributed to the growing sophistication and profitability of ransomware attacks targeting hospitals, financial institutions, government agencies, and critical infrastructure.

Hybrid warfare represents another area profoundly influenced by AI. Hybrid threats combine conventional military operations with cyber attacks, economic coercion, disinformation campaigns, psychological operations, and political interference. AI amplifies each component by enabling large-scale automation and personalization. Machine learning algorithms analyze demographic data, behavioral patterns, and online interactions to identify vulnerable audiences for influence operations. Deep learning techniques generate realistic synthetic media capable of impersonating political leaders, military officials, and journalists, thereby undermining public trust and complicating crisis management.

The proliferation of AI-generated disinformation presents a significant challenge to democratic governance. During periods of political tension or armed conflict, malicious actors may deploy deepfakes, automated social media accounts, and algorithmically optimized propaganda to manipulate public opinion, suppress voter participation, or exacerbate social divisions. Because AI-generated content is increasingly difficult to distinguish from authentic material, governments face growing difficulties in preserving information integrity without infringing upon freedom of expression. From a strategic perspective, AI-enabled cyber warfare blurs the traditional distinction between war and peace. States may engage in continuous low-intensity cyber operations below the threshold of armed conflict, conducting espionage, intellectual property theft, infrastructure reconnaissance, and influence campaigns without triggering conventional military responses. This "gray-zone" competition complicates deterrence because attribution remains uncertain and proportional responses are difficult to calibrate. These developments suggest that cyber warfare in the AI era is characterized less by isolated attacks than by persistent strategic competition across interconnected digital ecosystems. Consequently, national security policies must evolve beyond reactive cybersecurity measures toward

comprehensive strategies integrating technological innovation, cyber resilience, legal frameworks, international cooperation, and public awareness.

Comparative Analysis of Major AI Powers and Implications for National Security

United States: Maintaining Technological and Military Superiority

The United States remains the global leader in AI innovation due to its world-class research universities, advanced technology firms, defense-industrial base, venture capital ecosystem, and extensive federal investment in research and development. The National Security Commission on Artificial Intelligence (NSCAI, 2021) argued that AI will fundamentally reshape global power in much the same way that electricity and nuclear technology transformed previous eras. The U.S. Department of Defense has integrated AI into military modernization through initiatives such as the Joint All-Domain Command and Control (JADC2) architecture, Project Maven, autonomous systems development, and AI-enabled intelligence analysis. These initiatives aim to create seamless information sharing across the Army, Navy, Air Force, Marine Corps, Space Force, and Cyber Command, thereby accelerating battlefield decision-making.

The United States also recognizes AI as central to cybersecurity. Agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) increasingly employ AI for continuous threat detection, vulnerability management, and critical infrastructure protection. The release of Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence further demonstrates the government's commitment to balancing innovation with risk management. However, the United States faces several challenges. Rapid private-sector innovation often outpaces regulatory development, creating governance gaps. Additionally, concerns surrounding algorithmic bias, privacy, misinformation, and AI-enabled election interference remain significant policy issues.

China: Artificial Intelligence and Digital Sovereignty

China has adopted one of the world's most comprehensive AI strategies. The New Generation Artificial Intelligence Development Plan (State Council of China, 2017) established the objective of becoming the global AI leader by 2030. Unlike liberal democracies, China's AI strategy integrates economic development, military modernization, public administration, and social governance within a centralized political framework. AI supports extensive applications in facial recognition, smart cities, public surveillance, predictive policing, and digital governance. The People's Liberation Army (PLA) increasingly emphasizes "intelligentized warfare," in which AI supports

autonomous weapons, command systems, electronic warfare, cyber operations, logistics, and battlefield decision-making. Chinese military scholars argue that AI will determine future strategic superiority by enabling faster operational cycles and integrated information dominance.

China also strongly advocates the principle of cyber sovereignty, maintaining that every state possesses sovereign authority over its domestic cyberspace, internet governance, and digital infrastructure. This approach differs substantially from Western models favoring an open and globally interconnected internet. China's rapid progress in AI demonstrates how technological innovation can simultaneously strengthen state capacity while raising international concerns regarding surveillance, privacy, and geopolitical competition.

Russia: Artificial Intelligence as an Asymmetric Equalizer

Russia views AI primarily through the lens of strategic competition and military modernization. President Vladimir Putin famously remarked that "whoever becomes the leader in AI will become the ruler of the world," highlighting the perceived geopolitical importance of AI.

Russia's AI strategy focuses heavily on:

- autonomous military systems,
- electronic warfare,
- cyber operations,
- strategic intelligence,
- information warfare,
- unmanned combat vehicles.

Given economic constraints relative to the United States and China, Russia increasingly relies upon AI to offset conventional military disadvantages through asymmetric capabilities. Russian cyber operations have demonstrated the strategic utility of combining cyber attacks with information operations. Incidents involving election interference, infrastructure attacks, and coordinated disinformation campaigns illustrate how AI-enhanced cyber capabilities can influence geopolitical outcomes without conventional military confrontation.

European Union: Human-Centered Artificial Intelligence

The European Union adopts a distinctly different approach emphasizing ethical AI, human rights, transparency, and regulatory governance.

Rather than competing solely through military AI, the EU seeks to become the global standard-setter for trustworthy AI. The AI Act establishes a

comprehensive regulatory framework based upon risk categorization. High-risk AI applications—including those affecting critical infrastructure, healthcare, law enforcement, and border management—are subject to strict regulatory requirements. The EU simultaneously strengthens cybersecurity through the NIS2 Directive, the Cybersecurity Act, and coordinated digital resilience initiatives. This governance-oriented approach demonstrates that AI leadership may derive not only from technological capability but also from regulatory legitimacy and international norm entrepreneurship.

Israel: Innovation and Cybersecurity Leadership

Israel has emerged as one of the world's foremost cybersecurity powers despite its relatively small population.

Several factors contribute to Israeli success:

- close collaboration between military intelligence and private industry,
- significant investment in cybersecurity research,
- strong university-industry partnerships,
- thriving startup ecosystem,
- compulsory military service producing highly skilled cyber professionals.

Israeli AI applications extend across:

- missile defense,
- autonomous systems,
- intelligence analysis,
- cybersecurity,
- border surveillance,
- counterterrorism.

Israel demonstrates that technological innovation, rather than population size, increasingly determines cyber power.

India: AI for Strategic Autonomy and Development

India views AI as both a national development tool and a strategic capability. Through initiatives such as the National Strategy for Artificial Intelligence and Digital India, the country seeks to leverage AI across healthcare, agriculture, education, governance, and defense. India's emphasis on indigenous semiconductor production, digital public infrastructure, and AI research reflects broader ambitions to reduce dependence on foreign technologies and enhance technological sovereignty. While still confronting capacity and infrastructure

challenges, India's approach illustrates how emerging powers can integrate AI into long-term national development and security strategies.

Nigeria and Africa: Opportunities and Strategic Vulnerabilities

African countries increasingly recognize AI as an engine for socioeconomic transformation. The African Union's Continental AI Strategy and the African Union Convention on Cyber Security and Personal Data Protection provide important continental frameworks for responsible digital development. Nigeria has experienced rapid digital transformation through mobile banking, fintech innovation, e-government services, and expanding digital entrepreneurship. However, AI adoption remains constrained by inadequate digital infrastructure, unreliable electricity, limited research funding, shortages of AI specialists, fragmented cybersecurity governance, and dependence on imported technologies.

Cybercrime continues to impose substantial economic costs on Nigeria and other African economies. Critical sectors—including banking, telecommunications, energy, and public administration—remain vulnerable to ransomware, phishing, identity theft, and attacks on critical infrastructure. Despite these challenges, AI presents significant opportunities. Intelligent systems can strengthen border security, improve intelligence analysis, support precision agriculture, enhance healthcare delivery, optimize transportation, and improve public service delivery. To realize these benefits, African governments should prioritize investments in digital infrastructure, AI education, indigenous research, cybersecurity institutions, and regional cooperation. Building local capacity will be essential for safeguarding digital sovereignty and reducing strategic dependence on external technology providers.

Artificial Intelligence, Digital Sovereignty, and International Law

The rapid advancement of AI has exposed significant limitations within existing international legal frameworks. While the United Nations Charter, international humanitarian law, and the law of state responsibility provide general principles governing the use of force, they offer limited guidance regarding autonomous cyber operations, AI-enabled military systems, and algorithmic decision-making. A central challenge concerns attribution. Cyber operations frequently involve proxy actors, distributed infrastructure, and sophisticated techniques designed to conceal the origin of attacks. AI further complicates attribution by enabling automated attacks that evolve dynamically during execution. Determining legal responsibility under such circumstances remains difficult.

Another challenge relates to the principle of sovereignty. Traditional interpretations emphasize territorial integrity and non-intervention. However, cyber operations can disrupt critical infrastructure, manipulate information environments, and compromise governmental functions without crossing physical borders. Consequently, scholars increasingly argue that sovereignty must encompass control over digital infrastructure, strategic data, communication networks, and AI systems. The debate over Lethal Autonomous Weapons Systems (LAWS) illustrates broader governance challenges. While some states advocate legally binding restrictions on autonomous weapons, others emphasize the strategic advantages of continued technological development. The absence of international consensus raises concerns regarding arms races, accidental escalation, and accountability for AI-enabled military actions. These developments suggest that international law must evolve to address digital sovereignty, algorithmic accountability, responsible AI development, and norms governing cyber conflict.

Policy Implications

The findings of this study carry several important policy implications.

First, governments should treat AI as a strategic national capability comparable to energy security, nuclear technology, or critical infrastructure. National AI strategies should integrate defense, education, industry, research, and cybersecurity within a coordinated framework.

Second, cybersecurity policies must evolve from reactive incident response toward proactive cyber resilience. AI-enabled threat intelligence, continuous monitoring, and predictive analytics should become integral components of national cybersecurity strategies.

Third, investments in domestic research and development are essential for technological sovereignty. States that remain dependent on foreign AI platforms, cloud infrastructure, and semiconductor supply chains may face strategic vulnerabilities during periods of geopolitical tension.

Fourth, ethical AI governance should accompany technological innovation. Transparency, accountability, fairness, privacy protection, and human oversight are necessary to maintain public trust while reducing the risks associated with algorithmic bias and autonomous decision-making.

Finally, international cooperation remains indispensable. Cyber threats transcend national boundaries, making information sharing, joint capacity building, confidence-building measures, and multilateral norm development critical components of global security.

Conclusion

Artificial Intelligence has emerged as one of the most transformative forces shaping the contemporary international system. Its integration into military operations, cybersecurity, intelligence, governance, and economic development has fundamentally altered the meaning of power and the practice of national security. Unlike previous technological revolutions, AI simultaneously enhances state capabilities while creating new forms of vulnerability that transcend traditional territorial boundaries. This study has demonstrated that cyber power increasingly complements conventional military power as a central instrument of statecraft. AI amplifies cyber capabilities through automation, predictive analytics, adaptive learning, and large-scale data processing, enabling both state and non-state actors to conduct sophisticated operations across interconnected digital environments. Consequently, strategic competition now extends beyond physical domains into cyberspace, where information superiority, technological innovation, and digital resilience have become essential determinants of national power.

The comparative analysis of the United States, China, Russia, the European Union, Israel, India, and Nigeria reveals that states are adopting diverse approaches to AI governance and cyber strategy, reflecting their political systems, security priorities, and levels of technological development. Despite these differences, a common pattern emerges: technological leadership increasingly influences geopolitical influence, military effectiveness, and economic competitiveness. The study further argues that the traditional Westphalian conception of sovereignty is undergoing significant transformation. In the twenty-first century, sovereignty extends beyond territorial control to encompass authority over digital infrastructure, strategic data, communication networks, AI systems, and critical technologies. Digital sovereignty, therefore, has become an indispensable component of national security.

Looking ahead, the future international order will likely be shaped by the interaction between technological innovation, geopolitical competition, and international governance. States that successfully integrate AI with responsible governance, cybersecurity resilience, ethical standards, and international cooperation will be better positioned to safeguard their sovereignty and advance their national interests. Conversely, failure to adapt may expose nations to heightened strategic vulnerabilities in an increasingly interconnected and technologically competitive world. Artificial Intelligence should thus be viewed not merely as a technological innovation but as a transformative strategic capability that is redefining the foundations of state sovereignty, reshaping the

nature of conflict, and influencing the future architecture of international security.

Recommendations

Based on the analysis presented, the following recommendations are proposed:

1. Develop Comprehensive National AI Strategies**:** Governments should establish integrated AI policies that align technological innovation with national security, economic development, education, and digital governance.
2. Strengthen Cybersecurity Institutions: National Computer Emergency Response Teams (CERTs), cybersecurity agencies, and intelligence organizations should expand AI-enabled cyber defense capabilities and invest in workforce development.
3. Invest in Indigenous Research and Innovation**:** States should prioritize funding for AI research, semiconductor technologies, quantum computing, and advanced digital infrastructure to reduce strategic dependence on foreign technologies.
4. Enhance Critical Infrastructure Protection**:** Operators of energy, healthcare, finance, transportation, telecommunications, and water systems should deploy AI-driven monitoring and resilience measures to safeguard essential services.
5. Promote Ethical and Responsible AI**:** Governments should adopt regulatory frameworks that ensure transparency, accountability, human oversight, and protection of fundamental rights in AI deployment.
6. Strengthen International Cooperation**:** Regional and global organizations should promote information sharing, harmonized cybersecurity standards, and collaborative research to address transnational cyber threats.
7. Develop AI Talent and Digital Literacy**:** Investments in education, professional training, and interdisciplinary research are essential for building a sustainable AI workforce and enhancing national resilience.
8. Support African Digital Sovereignty**:** African states should strengthen regional cooperation through the African Union and Regional Economic Communities to develop shared cybersecurity capabilities, harmonized legal frameworks, and indigenous AI innovation ecosystems.

Author Contributions

Francis C. Okpo: Conceptualization, Methodology, Writing – review & editing, Supervision, Project administration. **Mukhtar Imam**: Methodology, Writing – review & editing, Investigation. **Joseph O. Odama**: Conceptualization, Methodology, Writing – review & editing, Investigation.

Acknowledgement

The authors would like to express their sincere appreciation to the editorial team and reviewers of Multidisplinary Bulletin of Global Scholarship for their constructive comments, insightful suggestions, and professional guidance throughout the review process. Their valuable feedback has significantly contributed to improving the quality, clarity, and scholarly contribution of this manuscript. The authors also acknowledge the academic environment and institutional support that facilitated the completion of this research. Appreciation is extended to colleagues and scholars who provided intellectual discussions and valuable input during the development of this study. Finally, the authors are grateful to all researchers whose works were included in the bibliometric dataset, as their scholarly contributions form the foundation for advancing interdisciplinary knowledge and enabling this analysis of research trends.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

Use of artificial intelligence (AI)

The authors declare that no generative artificial intelligence (AI) tools were used in the preparation, analysis, or writing of this manuscript

Bibliography

1) Aldrich, R. J., & Karatzogianni, A. (2025). Cyber Power and Cyber Diplomacy. In The Palgrave Handbook on Cyber Diplomacy (pp. 53–75). Springer Science+Business Media. https://doi.org/10.1007/978-3-031-93385-1_3
2) Bernhardt, W., Duvenage, P., & von Solms, S. (2026). African Cyber Power: Establishing a Strategic Rationale for Offensive Cyber Capabilities - The Case of South Africa. In M. J., P. J., K. M., M. W., T. K.-L., F. L., & J. van V. J. (Eds.), IFIP Advances in Information and Communication Technology:

Vol. 777 IFIPAICT (pp. 81–93). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-032-13075-4_6

3) Bernhardt, W., Duvenage, P., & Von Solms, S. (2025). Configuration of African Cyber Power: Three Conceptual Precepts. In L. C. & H. B. (Eds.), European Conference on Information Warfare and Security, ECCWS (pp. 36–41). Curran Associates Inc. https://doi.org/10.34190/eccws.24.1.3429
4) Berrefjord, V. R., & Bjørstad, T. E. (2025). Commercially sourced intelligence: friend or foe? Intelligence and National Security, 40(3), 391–411. https://doi.org/10.1080/02684527.2024.2437955
5) Devanny, J., & Dwyer, A. C. (2023). From Cyber Security to Cyber Power: Appraising the Emergence of "Responsible, Democratic Cyber Power" in UK Strategy. In J. T., G. C.D., P. K., & W. I. (Eds.), International Conference on Cyber Conflict, CYCON (Vols. 2023-May, pp. 381–397). NATO CCD COE Publications. https://doi.org/10.23919/CyCon58705.2023.10181804
6) Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). The rise of cyber power in Brazil. Revista Brasileira de Politica Internacional, 65(1). https://doi.org/10.1590/0034-7329202200113
7) Duvenage, P., Bernhardt, W., & Von Solms, S. (2023). Cyber power in the african context: An exploratory analysis and proposition. In A. A. & D. C. (Eds.), European Conference on Information Warfare and Security, ECCWS (Vols. 2023-June, pp. 177–186). Curran Associates Inc. https://www.scopus.com/pages/publications/85167602619?origin=resultslist
8) Hardy, A. (2025). RUSSIAN CYBER POWER IN THE BALTIC STATES: LESSONS FROM THE FRONTLINE OF DEMOCRACY. In The Anthem Handbook of Soft Power and Public Diplomacy in the Age of AI (pp. 295–312). Anthem Press. https://www.scopus.com/pages/publications/105040314616?origin=resultslist
9) Hermida, Y. G. (2026). The Quest for Cyber Power: The Evolution of China's Cyber Strategy. Journal of Asian Security and International Affairs, 13(2), 139–160. https://doi.org/10.1177/23477970261424600
10) Kasper, A., & Vernygora, V. (2021). The EU's cybersecurity: A strategic narrative of a cyber power or a confusing policy for a local common market? Cuadernos Europeos de Deusto, 65, 29–71. https://doi.org/10.18543/CED-65-2021PP29-71
11) Khoirunnisa, K., Rahmadan, Y., & Jubaidi, D. (2025). Cyber Warfare and National Security: Modernizing Defense Strategies in the Context of China's Evolving Cyber Influence. China Quarterly of International Strategic Studies, 11(1), 1–20. https://doi.org/10.1142/S2377740025500010

12) Mattila, J. K. (2022). A Model for State Cyber Power: Case Study of Russian Behaviour. In E. T., K. N., O. C., & O. C. (Eds.), European Conference on Information Warfare and Security, ECCWS (Vols. 2022-June, pp. 188–197). Curran Associates Inc. https://www.scopus.com/pages/publications/85172885247?origin=resultslist
13) Mustafa, H. M., Bariya, M., Sajan, K. S., Chhokra, A., Srivastava, A., Dubey, A., Von Meier, A., & Biswas, G. (2021). RT-METER: A real-time, multi-layer cyber-power testbed for resiliency analysis. 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2021, Held as Part of the Cyber-Physical Systems and Internet-of-Things Week, Proceedings. https://doi.org/10.1145/3470481.3472708
14) Pačka, R., & Mareš, M. (2023). Achieving Cyber Power Through Integrated Government Capability: Factors Jeopardizing Civil-Military Cooperation on Cyber Defense. Journal of Applied Security Research, 18(3), 436–461. https://doi.org/10.1080/19361610.2021.2006033
15) Phahlamohlaka, J., Ngobeni, S., & Baloyi, B. (2024). The Relevance of Cyber Diplomacy to Arguments about National Cyber Power. Global Congress on Emerging Technologies, GCET 2024, 101–106. https://doi.org/10.1109/GCET64327.2024.10934674
16) Realpe Díaz, M. E. (2024). Cyber Diplomacy in Cyber Power: Mechanisms and Strategies for Furthering National Interests. Novum Jus, 18(2), 279–304. https://doi.org/10.14718/NovumJus.2024.18.2.11
17) Sarker, P. S., Patari, N., Ha, B., Majumder, S., & Srivastava, A. K. (2022). Cyber-Power Testbed for Analyzing Distributed Control Performance during Cyber-Events. 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems, MSCPES 2022. https://doi.org/10.1109/MSCPES55116.2022.9770160
18) African Union. (2024). *Continental Artificial Intelligence Strategy*. Addis Ababa: African Union Commission.
19) Brundage, M., Avin, S., Clark, J., et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford.
20) Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.
21) Carr, E. H. (1939). *The twenty years' crisis, 1919–1939*. Macmillan.
22) Horowitz, M. C. (2018). *Artificial intelligence, international competition, and the balance of power*. Texas National Security Review, 1(3), 36–57.
23) Jervis, R. (1978). Cooperation under the security dilemma. *World Politics, 30*(2), 167–214.

24) Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? *Business Horizons, 62*(1), 15–25.
25) Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.
26) Kissinger, H., Schmidt, E., & Huttenlocher, D. (2021). *The age of AI: And our human future*. Little, Brown.
27) Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.
28) Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.
29) McCarthy, J. (1956). *The Dartmouth Summer Research Project on Artificial Intelligence*. Dartmouth College.
30) Morgenthau, H. J. (1948). *Politics among nations*. Alfred A. Knopf.
31) National Security Commission on Artificial Intelligence. (2021). *Final report*. Washington, DC.
32) Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace*. *International Security, 41*(3), 44–71.
33) Nye, J. S. (2024). *A life in the American century*. Polity Press.
34) O'Neil, C. (2016). *Weapons of math destruction*. Crown.
35) Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
36) Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton.
37) Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar*. Oxford University Press.
38) State Council of China. (2017). *New generation artificial intelligence development plan*. Beijing.
39) United States Department of Defense. (2023). *Data, analytics, and artificial intelligence adoption strategy*. Washington, DC.
40) Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.
41) Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Copyright