TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

TECHNOLOGICAL COERCION AS STATECRAFT: HOW CONTROL OVER EMERGING TECHNOLOGIES IS RECONFIGURING THE GLOBAL MILITARY BALANCE OF POWER

Maria CONSTANTINESCU, Paul TUDORACHE

Abstract: *This paper addresses the issue of technological coercion (the strategic use of control over critical technologies to exert geopolitical influence) as a defining element of 21st-century statecraft and military power. The authors employ a qualitative, case-study-driven framework to analyze how dominance in AI, data infrastructure, autonomous systems, and semiconductor supply chains has become a primary instrument of coercion, enabling states to project power without direct conflict. The analysis reveals that technological dependency creates asymmetric leverage, operational vulnerability, and a new form of "algorithmic colonialism." The paper concludes with a preview of eight strategic recommendations for nations to build resilient and sovereign tech ecosystems, enforce algorithmic transparency, and reform international law to counter AI-driven coercion.*

Keywords: *Technological coercion, Data sovereignty, AI in warfare, DIME-T framework, Algorithmic control, Autonomous systems, Technological statecraft.*

1. INTRODUCTION

While military force and economic sanctions remain potent tools of national power, a new and arguably more decisive form of influence is emerging: technological coercion, understood as the strategic use of control over critical technologies though a variety of means, such as export controls, investments in selective industries, investment screening, supply chain manipulation, and standards-setting to exert geopolitical influence by rewarding allies, punish rivals, and shaping the strategic environment. The traditional technological diplomacy of negotiating scientific cooperation or managing technology transfer agreements is increasingly being replaced by a more assertive and often coercive strategy, where control over critical technologies (from semiconductors and quantum computers to artificial intelligence and the algorithms that shape public discourse) is wielded as a primary instrument of geopolitical power. The main argument of the paper is that the strategic control of technology has become a new and potent form of statecraft, fundamentally reconfiguring the global military balance of power and challenging the foundations of the post-Cold War international security system.

This paper employs a qualitative, case-study-driven framework to analyze how control over emerging and disruptive technologies (including AI, autonomous systems, semiconductors, and quantum computing) is leveraged by state and non-state actors to exert geopolitical coercion. The analysis synthesizes evidence from publicly available government documents, policy reports, academic literature, and verified media sources to trace patterns of technological dependency, strategic denial, and infrastructure-based leverage across three domains.

This research provides an analytical framework for understanding technological competition as a primary driver of geopolitical conflict, with direct applications across multiple domains. In International Security and Strategic Studies, it offers scholars and policymakers a unified model for analyzing how states wield technological control as an instrument of power.

In Defense Policy and Planning, military organizations can use this framework to inform capability development, R&D priorities, procurement strategies, and technological partnerships, recognizing that technological superiority now depends on ecosystem resilience and sovereignty, not merely platform performance. In Foreign Policy and Diplomacy, the framework helps policymakers to identify technological coercion, build counter-coalitions, and engage in strategic technological diplomacy. In geo-economics, it demonstrates how trade policy, investment screening, and industrial strategy function as instruments of geopolitical power.

From a technological perspective, it enables the identification of emerging technological vulnerabilities across semiconductors, quantum computing, artificial intelligence, and cybersecurity infrastructure, offering guidance on standards-setting as a strategic tool and on the militarization of dual-use technologies. Also, it allows defense planners and policymakers to anticipate how technological competition will reshape military capabilities, alliance structures, and strategic stability. By synthesizing these technological dimensions into a coherent strategic framework, the paper provides guidance for intelligence analysts tracking technological threats, military strategists planning for future conflicts, government leaders making technology policy decisions, and academics building next-generation international relations theory.

The problem facing the international security system is twofold. As one of the authors argued in another paper [1], the traditional understanding of national power (based on military capability, economic strength, and soft power) in the framework of DIME, should be extended to DIME-T, to include the technological factor. A nation's strategic position will increasingly be determined by its position within fragmented technological ecosystems and its ability to control the creation, flow, and utilization of critical technologies. Secondly, the mechanisms through which this new form of power (technological coercion) is exercised are complex and not yet well understood by policymakers and defense planners. The factors underlying technological coercion include a combination of state and private actors, technical aspects difficult to grasp by the non-specialists, a rapidly evolving ecosystem which moves at a speed to which the traditional decision making processes are not accustomed to and the development of specific research and business environments. Without a clear analytical framework to identify and understand these mechanisms, significant financial investments and changes in the legislative frameworks, and most importantly a change is mindset, nations and alliances are ill-equipped to navigate this new, contested technological landscape.

Figure 1 illustrates the analytical framework on explored throughout this paper, mapping the relationship between the DIME-T model and the mechanisms of technological coercion that will be examined in the subsequent sections

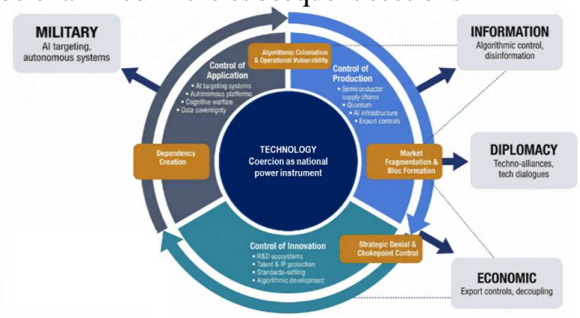


Fig. 1. Technology coercion in the framework of DIME-T model

2. BRIEF LITERATURE REVIEW

The existing scholarship on technological competition and geopolitical power can be approached from four interconnected directions of research. The first addresses the US-China strategic rivalry through a historical lens. Graham Allison's work on the "Thucydides Trap" provides a framework for understanding how rising powers challenge established ones, a dynamic now playing out in the technological domain [2]. Allison argues that power transitions create structural instability, with technology becoming the primary arena of competition [3].

The second direction focuses on supply chain security and technological chokepoints, with Gregory C. Allen and his colleagues have documented how control over semiconductor supply chains has become central to national

security and artificial intelligence development, demonstrating that technological vulnerability is a direct security threat, shifting policy discussions from free trade to strategic autonomy [4]. Dimitri Alperovitch, co-founder of CrowdStrike and leading expert on cyber threats, has extended this analysis to demonstrate how technological competition extends beyond semiconductors to encompass cybersecurity infrastructure and the weaponization of digital systems as tools of statecraft [5]. In his seminal book [6], Alperovitch outlines how the technological competition between the United States and China, combined with emerging cyber threats and the militarization of digital infrastructure, is creating unprecedented strategic instability. His work reveals how technological coercion operates simultaneously through the kinetic and cyber domains and the manner in which the fragmentation of global technology markets is fundamentally reshaping the international security landscape.

The third direction examines technological sovereignty and data governance and the manner in which nations assert control over digital infrastructure, algorithms, and data flows as instruments of power, focused on the TikTok debate, the European Digital Services Act, and China's data localization requirements all reflect this emerging concern [7][8]. A research gap which emerges from the study of this particular literature refers to the manner in which algorithmic sovereignty is treated as separate from semiconductor competition or quantum computing races, missing the interconnected geopolitical and economic dynamics that underpin all three domains. This siloed approach overlooks how control over foundational technologies collectively shapes national and corporate power in the digital age.

The fourth direction addresses emerging and disruptive technologies as vectors of geopolitical power. Dong and Mcintyre have analyzed how artificial intelligence and automation are reshaping economic power and creating new dependencies between nations [9]. Their work demonstrates that control over AI capabilities is becoming as strategically important as control over traditional energy resources. Similarly, Kai-Fu Lee has documented how China's approach to AI development differs fundamentally from the West, emphasizing state coordination and strategic integration with military applications [10]. Toby Ord's work on existential risks from emerging technologies highlights how quantum computing, synthetic biology, and advanced AI represent not merely economic opportunities but potential instruments of unprecedented strategic power [11].

While the existing research provides valuable insights, it remains largely stove-piped, failing to synthesize these phenomena into a unified theory of technological coercion as statecraft. Analyses focus on specific technologies, bilateral competitions, or individual policy mechanisms without recognizing they are interconnected elements of a coherent global strategy.

This paper addresses this gap by proposing that technological coercion operates across three integrated domains (control of production, control of innovation, and control of application) and that understanding this unified phenomenon is essential for navigating 21st-century international security.

3. THE DAWN OF THE TECHNOLOGICAL COERCION ERA

The post-Cold War era was characterized by a broad consensus among developed nations that technology markets should be liberalized, that scientific cooperation should be encouraged across borders, and that the free flow of information and innovation would benefit all parties. This consensus was reflected in the creation of the World Trade Organization, the proliferation of bilateral and multilateral trade agreements, and the emergence of global supply chains that integrated production across dozens of countries. Technology companies were encouraged to source components globally, establish research centers in multiple countries, and collaborate with international partners. This system was based on the assumption that economic interdependence would reduce the likelihood of conflict and that technological progress would be a shared good, advancing human welfare universally.

This long-held consensus is now breaking down, driven by a combination of factors: China's rise as a technological power, the acceleration of technological change led by private companies enabling them to become actors on the geopolitical scene, the growing recognition that emerging technologies have direct military applications and, most importantly, the return to peer-competition and the dissolution of the geo-political and economic post-World War II order.

The United States, in particular, has begun to view technology not as a commodity to be traded freely but as a strategic asset to be protected and leveraged for national advantage. Similarly, China has pursued a deliberate strategy of technological self-sufficiency, seeking to reduce its dependence on Western technology while simultaneously acquiring foreign technological capabilities through investment, espionage, and talent recruitment.

We are moving forward towards an era of selective decoupling, characterized by the deliberate fragmentation of the global technology market into distinct, competing blocs, driven by the national security imperatives of major powers. This fragmentation is not a temporary phenomenon or a negotiating tactic, it reflects a fundamental change in how nations view the relationship between technology and power.

The core of this new doctrine is *technological coercion*, apparent in four primary ways. First, ***selective decoupling,*** involving the deliberate fragmentation of technology supply chains, most notably in the semiconductor industry, with United States and China actively working to reduce their mutual dependencies. Rather than maintaining a single, globally integrated supply chain, nations are now deliberately creating parallel ecosystems isolated from competitors.

Second, ***algorithmic sovereignty*** disputes emerge as conflicts over the control of data and algorithms that influence populations, as exemplified by international debates surrounding platforms like TikTok.

Third, ***weaponization of standards*** signifying the development and use of technical standards, particularly in emerging fields like quantum computing, as a geopolitical tool to gain control over the technological advantages and create dependencies.

Fourth, ***techno-economic bloc formation*** through the rise of new alliances, such as BRICS, that integrate military and technological cooperation to challenge the existing international order.

The impact of this new reality is profound, creating new strategic vulnerabilities for all nations, destabilizing traditional alliances caught between competing technological ecosystems, and introducing new vectors for conflict. The very nature of warfare and national power is being redefined, shifting from the focus on traditional military platforms towards the control of the underlying technological infrastructure that enables modern military and economic power.

4. THE DOCTRINE OF TECHNOLOGICAL COERCION

Recent events illustrate that technology is no longer just a tool for achieving military objectives, becoming a tool for strategic coercion and the exercise of diplomatic power.

One area which has become a defining criterion of national power is the ***ability to control sovereign AI models and data.*** The United States, India, and China exemplify three distinct approaches to achieving AI sovereignty, reflecting their specific geopolitical position and strategic objectives. The United States has prioritized building domestic AI infrastructure through massive capital investments, most notably the Stargate Project [12], a $500 billion public-private partnership backed by OpenAI, SoftBank, and Oracle, designed to establish five AI computing sites across the country and secure American technological dominance, by ensuring that "US technology and US standards, particularly in AI, biotech, and quantum computing, drive the world forward" [13]. India launched its sovereign large language model initiative, developed by a private startup Sarvam AI with state support. The model is designed to be open-source, with 120 billion parameters, trained on Indian language datasets, and optimized for voice-enabled applications and digital governance, reflecting the "self-reliant

India" objective to mitigate geopolitical shocks and protect national values from foreign influence [14]. China has been actively pursuing a comprehensive strategy of "independent and controllable" AI development across the entire technology stack, combining state support for semiconductor manufacturing (led by Huawei), domestically developed machine learning frameworks, and competitive large language models like DeepSeek [15]. Another recent example is the joint public-private initiative to build a sovereign AI infrastructure for public administration by France and Germany, explicitly framed as a survival necessity with the aim of reducing European dependence on non-European technology providers. This initiative treats AI not just as software, but as sovereign infrastructure equivalent to energy or defense [16]. This competition reflects a fundamental shift in technological power, which is no longer about access to superior technology, but about building and controlling AI systems that serve national interests while remaining insulated from external coercion, creating a hierarchy of technological access and forcing smaller countries to choose between competing U.S. and Chinese ecosystems.

Another area of control refers to ***critical semiconductor assets.*** The U.S., citing national security concerns, ordered HieFo Corporation, a US-based firm controlled by a Chinese national, to divest its 2024 acquisition of EMCORE's semiconductor assets (particularly chips critical to defense navigation systems), fabrication and processes business, citing national security risks related to the transfer of proprietary technology to China, despite the company's U.S. incorporation [17]. This action illustrates the degree to which the U.S. government is willing to intervene in the technology market, extending far beyond traditional export controls to encompass investment screening and corporate restructuring.

In a strategic countermove, China launched a formal investigation into Meta's $2 billion acquisition of Singaporean AI startup Manus to assess potential violations of its export control laws, arguing that the AI technology originated in China and should not be transferred abroad without authorization [18]. The investigation signaled China's determination to prevent its domestic innovators from fleeing to the U.S. States after benefiting from national talent pools and policy support.

State actors are not the only ones contributing to the emergence of technological coercion, as powerful private actors exert their influence over states to promote their business interests. Following the European Commission's €120 million fine against X for violating the Digital Services Act, Elon Musk publicly denounced the EU, calling for its abolition and comparing its regulators to fascist figures. His rhetoric was echoed and amplified by top officials in the Trump administration, including Secretary of State Marco Rubio, who labeled the fine an "attack on all American tech platforms and the American people by foreign governments", while the U.S. Trade Representative subsequently threatened retaliatory countermeasures against European service providers, signaling a coordinated political response [19].

Quantum computing is treated by the U.S. and China as a top national priority, central to their military and strategic advantage, resulting in significant investments supporting the development of a "crypto-analytically relevant" quantum computer, allowing the decryption of decades of stored intelligence data [20]. China is pursuing technological autonomy through heavy R&D investment, developing both quantum computing and quantum-resistant cryptography and launching its own national standardization process aimed at migrating critical infrastructure to quantum-resistant systems [21].

Algorithmic sovereignty is another pillar of technological coercion. When a nation cannot audit, modify, or regulate the algorithms shaping its citizens' information environment, it loses control over its digital public sphere, generating a vulnerability that can be weaponized by foreign actors, hostile states, or even domestic bad actors with access to algorithmic tools. Various reports have documented how foreign actors exploited algorithmic control over social media platforms to influence elections. For instance, Russian operatives used Facebook's and Twitter's recommendation algorithms, which prioritize engagement, to amplify divisive content, fake

news, and targeted political ads. Although the platforms were U.S.-based, the algorithmic logic (owned and controlled by the platforms' parent companies) was not subject to external oversight or national regulation [22].

Regaining algorithmic sovereignty is not easy, as demonstrated by the US government attempt to regain control over the Chinese owned TikTok platform through the creation of a joint venture, a compromise that still leaves substantial technological control in the hands of ByteDance, which retains exclusive ownership of the algorithm [23].

These actions are not isolated incidents but rather manifestations of a new geopolitical doctrine where technology is no longer a neutral commodity but a strategic asset to be protected, cultivated, and, when necessary, denied to adversaries.

A new category of geopolitical risk emerges as another pillar of technological coercion, ***the fragmentation of the global technology market*** into distinct blocs. The United States is pursuing a strategy of "purging" Chinese influence from its semiconductor supply chain and restricting Chinese access to advanced technologies [24], while China is tightening its grip on artificial intelligence intellectual property and pursuing technological self-sufficiency in critical domains like quantum computing, semiconductors, and advanced manufacturing [25]. Europe, caught between these two superpowers, is attempting to develop its own technological capabilities and maintain relationships with both the United States and China [26], while other nations are making strategic choices about which technological bloc to align with nations [27]. This is not a temporary disruption, but a structural realignment, which introduces new vulnerabilities: operational dependency, algorithmic colonialism, and the weaponization of standards and supply chains. Nations that trade sovereignty for efficiency risk becoming subject to coercion, whether through restricted access to AI models, algorithmic manipulation, or cyber-enabled infrastructure control.

This fragmentation leads to increased cost of innovation, by reducing the scale of markets, fragmenting supply chains and changing the assumptions that companies can source components globally or collaborate with researchers worldwide. It also creates redundancy and inefficiency, as different blocs develop parallel technological capabilities and increases the risk of technological conflict, as nations compete for dominance in critical technologies and attempt to deny capabilities to their rivals.

5. THE EXPANSION OF TECHNOLOGICAL COERCION MILITARY DOMAINS

The future warfare will most likely be heavily dependent on technology, and the deliberate denial, conditioning, or control of access to critical technologies (from hardware, software, data infrastructure, algorithmic capability, intelligence or Starlink satellite service) will increasingly be used as a tool in hybrid warfare. Technological asymmetry will increasingly be leveraged to create coercive advantage without triggering formal declarations of conflict.

AI-Driven Targeting Systems, such as the U.S. Project Maven, provide useful insights into the future operational environment. Project Maven uses machine learning to rapidly analyze battlefield reconnaissance data (including video, satellite, and radar feeds) to identify, categorize, and recommend engagement strategies for targets like tanks or radars, operating with human oversight. Its effectiveness was successfully tested in real-world conflicts in Syria and Ukraine [28]. Beyond its undeniable value as a force multiplier, its strategic value as a tool of technological coercion lies also in its proprietary architecture and algorithmic opacity. Once integrated into command systems, it creates operational dependency, making it politically and logistically difficult for partner nations to exit or audit the system. Allies that adopt Maven-like platforms cede not just data, but control over targeting logic, often without access to source code, training data, or update protocols, actually outsourcing sovereign decision-making to algorithms governed by foreign entities creating a subtle but powerful lever of influence. The U.S. retains the ability to condition access, for example by restricting export of the underlying AI models,

limiting integration with non-U.S. systems, or updating algorithms to prioritize U.S. intelligence objectives.

While AI targeting systems like Maven reshape battlefield decisions through algorithmic speed and precision, a deeper and more insidious form of technological coercion emerges, ***cyber coercion via infrastructure control,*** when states gain control over the very infrastructure that enables those decisions, turning cloud platforms, communication networks, and data pipelines into levers of strategic pressure.

This can take the form of cyberattacks, like Russia's 2022 cyberattacks on Ukrainian power grids and communication networks [29] and the more recent cyberattacks targeting Poland's energy infrastructure designed to break morale and force political concessions [30] or the form of using the dominance in a specific infrastructure area for coercion. China is actively using dominance in 5G infrastructure (via Huawei), to achieve potential leverage over allied nations' military logistics and intelligence flows [31].

Algorithmic Propaganda and Cognitive Warfare represent a new frontier of military coercion, where AI-generated disinformation (such as deepfake videos, synthetic audio, and hyper-targeted content) is deployed to manipulate enemy populations, demoralize troops, or disrupt command structures. The Russian use of fabricated surrender orders during the Ukraine war exemplifies how algorithmic content can be weaponized for psychological effect, especially when hosted on civilian platforms that obscure attribution and evade regulation [32]. This mirrors broader vulnerabilities exposed in electoral contexts [33], where foreign actors exploited social media algorithms to amplify division and evade oversight. Electoral manipulation via algorithms can be viewed as technological coercion because it exploits foreign-controlled, opaque systems to distort public perception and behavior, denying sovereign states control over their democratic processes without firing a shot.

Naval and space domains are increasingly becoming arenas for technological coercion through the deployment of ***AI-powered autonomous systems***. Unlike traditional warfare, where human crews operate vessels or satellites, modern militaries are fielding AI-driven platforms that can patrol, surveil, intercept, or even engage targets without direct human control, enabling persistent, scalable, and deniable forms of pressure and introducing new coercive dynamics: presence without personnel, persistent surveillance without diplomatic footprint, and escalation without attribution.

In the maritime domain, the U.S. Navy's "Ghost Fleet Overlord" initiative deploys unmanned surface vessels to conduct persistent anti-submarine patrols and surveillance in contested zones such as the South China Sea. This enables a low-risk, continuous deterrence that pressures adversaries without risking human lives or triggering diplomatic escalation [34]. In space, China has advanced AI-powered reconnaissance satellites and co-orbital robotic platforms to autonomously track and potentially threaten foreign assets, including U.S. reconnaissance satellites, as demonstrated by a 2023 close-approach maneuver interpreted as a coercive signal [35]. These developments enable states to project power continuously, operate with deniability, and avoid attribution, fundamentally altering escalation dynamics. The strategic implications include persistent operational pressure on adversaries, asymmetric access for smaller actors, and critical legal gaps, as existing international frameworks were not designed to govern AI-driven coercion.

A parallel and equally potent form of technological coercion emerges in the realm of ***data sovereignty***. In the context of coercion, control over data infrastructure is not merely about privacy or efficiency, but about who can access, analyze, and act upon strategic information. A relevant example is Palantir, which integrates and fuses structured and unstructured data from diverse sources (including government intelligence, military logistics, biometric records, surveillance feeds, public health systems, financial transactions, and commercial satellite imagery) into its proprietary platforms (Gotham and Foundry), enabling AI-powered analysis and decision-making while often limiting client oversight, auditability, and data portability [36]. The company pursued an

aggressive policy of convincing European countries to adopt its platforms [37], with mixed results as some of the potential clients are beginning to realize its drawbacks. Switzerland explicitly rejected proposals to adopt Palantir's software for military intelligence, citing concerns over data sovereignty, transparency, and foreign dependency.[38]. Palantir's proprietary architecture makes migration nearly impossible, while its algorithms, inaccessible to clients, can be updated or influenced remotely, making the platform a tool for U.S. or Palantir's strategic interests. This creates asymmetric leverage, as nations relying on Palantir for mission-critical operations become subject to U.S. export controls, legal frameworks or even unannounced algorithmic shifts, effectively turning data infrastructure into a tool of geopolitical pressure.

6. CONCLUSIONS

The technologies outlined above reveal a new paradigm of military power: technological coercion is no longer about who has the most weapons, but who controls the algorithms, infrastructure, and cognition that shape the battlefield. Nations that fail to assert sovereignty over the technological domains (through regulation and domestic innovation) risk becoming subject to coercion by those who do.

To navigate this new era in which whoever controls the data infrastructure controls the future of governance, the following strategic recommendations should be addressed:

1. ***Adopt the DIME-T Framework*** **Integrate *Technology*** as a core pillar of national power alongside Diplomacy, Information, Military, and Economic tools, with defense and foreign policy institutions institutionalizing technological sovereignty as a strategic priority and not a technical afterthought.
2. ***Build Sovereign Data & AI Infrastructure*** Investing in nationally controlled, open-source, and interoperable platforms for defense and public administration (e.g., EU's GAIA-X, India's ONDC, or national AI stacks) is crucial, as is avoiding the over-reliance on foreign proprietary systems like Palantir, which embed long-term dependencies.
3. ***Enforce Algorithmic Auditing & Transparency*** Appropriate measures should be taken to mandate access to source code, training data, and to update protocols for any AI system integrated into national security or critical infrastructure, implementing third-party audits and establishing national algorithmic oversight bodies.
4. ***Strengthen Export Control & Investment Screening*** Expanding the regulatory frameworks to cover not just hardware, but software, data flows is another desirable step, along with treating algorithmic capabilities, AI models, cloud platforms, and data architectures as dual-use technologies subject to national security review.
5. ***Form Technological*** Alliances Coalitions based on shared technological values to counter coercive monopolies should be developed, and new tech dialogues, and regional innovation blocs should be formed, prioritizing interoperability without dependency.
6. ***Invest in Domestic Innovation Ecosystems*** Redirecting R&D funding toward critical technologies with dual-use potential should also be prioritized, along with measures to support domestic startups, talent retention, and public-private partnerships to reduce reliance on foreign innovation hubs.
7. ***Develop Legal Frameworks for AI-Driven Coercion*** Updating the international legal framework to address autonomous systems, algorithmic warfare, and data coercion is another recommendation, through the establishment of norms for attribution, accountability, and redress in cases of algorithmic manipulation or infrastructure sabotage.
8. ***Educate Policymakers & Military Leaders on Tech Literacy*** A final and most important recommendation is to introduce mandatory training on AI, data sovereignty, and cyber-physical systems for senior defense and diplomatic officials, allowing decision-

making to keep pace with the speed and complexity of technological change.

Failure to act will leave states vulnerable not to invasion, but to algorithmic subjugation, data captivity, and infrastructural coercion. These are silent, scalable, and deniable forms of pressure that redefine what it means to be powerful or powerless in the age of technological statecraft.

7. REFERENCES

[1] Constantinescu, M., *The National Security Strategy in the Current Environment: from DIME to a DIME-T Approach,* International Conference Knowledge-Based Organization Proceedings 27, 20-25, 2021, DOI: 10.2478/kbo-2021-0004.

[2] Allison, G., *Destined for War: Can America and China Escape Thucydides's Trap*, Houghton Mifflin Harcourt, 2017.

[3] Allison, G., Klyman, K., Barbesino, K., & Yen, H., *The Great Tech Rivalry: China vs. the U.S.,* Belfer Center for Science and International Affairs, 2021.

[4] Allen, G. C., Benson, E., Reinsch, W. A., *Improved Export Controls Enforcement Technology Needed for US National Security*, Center for Strategic International Studies, 2022, https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

[5] Alperovitch, D., *Eternal Vigilance: The Battle to Protect America from Cyber Attacks,* Broadside Books, 2022.

[6] Alperovitch, D., *World on the Brink: How America Can Beat China in the Race for the Future*, Broadside Books, 2024.

[7] Zuboff, S., *The Age of Surveillance Capitalism*, New York Public Affairs, 2019

[8] Yeung, K., *Hypernudge: Big Data as a mode of regulation by design,* Information, Communication & Society, 20:1, 118-136, 2017, DOI: 10.1080/1369118X.2016.1186713

[9] Dong, X., Mcintyre, S., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. Quantitative Finance, 14 (11), 2014, DOI: 10.1080/14697688.2014.946440.

[10] Lee, K. F., *AI Superpowers: China, Silicon Valley, and the New World Order*, Houghton Mifflin Harcourt, 2018.

[11] Ord, T., *The Precipice: Existential Risk and the Future of Humanity*. Hachette Book Group, 2020

[12] Open AI, *Announcing the Stargate Project*, 2025, https://openai.com/index/announcing-the-stargate-project/

[13] *National Security Strategy of the United States of America*, 2025, https://shorturl.at/UHc4p

[14] Sarvam, https://www.sarvam.ai/indias-sovereign-large-language-model.

[15] Chang, W., Arcesati, R., Hmaidi, A., *China's drive toward self-reliance in artificial intelligence: from chips to large language models*, MERICS Report, 2025, https://shorturl.at/2ZaHv.

[16] German Federal Ministry for Digital Transformation and Government Modernisation, *France and Germany Join Forces with Mistral AI and SAP SE to Launch a Sovereign AI for Public Administration*, Press Release, 2025 https://shorturl.at/sR8DI.

[17] White House, *Executive Order Regarding the Acquisition of Certain Assets of Emcore Corporation by Hiefo Corporation*, 2026, https://shorturl.at/aWFSM

[18] Siqi,J., Jiang, B., Chow, V., Feng, C., *China to probe Meta's purchase of Manus over export controls, tech outflow concerns*, The South China Morning Post, 2026, https://shorturl.at/AI8DQ

[19] Munster, B., *Musk threatens 'response' against individuals who imposed €120M X penalty*, Politico, 2025, https://shorturl.at/w4YIe

[20] Lague, D., *U.S. and China race to shield secrets from quantum computers*, Reuters, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-quantum/

[21] Swayne, M., *China Launches Its Own Quantum-Resistant Encryption Standards, Bypassing US Efforts*, Quantum Insider, 2025, https://shorturl.at/nD4RY

[22] Ribeiro, F. et al, *On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook*. 140-149, 2019. DOI: 10.1145/3287560.3287580.

[23] Wang, S., *Experts say banning TikTok won't solve security concerns*, 2024, https://shorturl.at/Da8sX

[24] US Department of Commerce, *FACT SHEET: President Biden Takes Action to Protect American Workers and Businesses from China's Unfair Trade Practices*, 2024, https://shorturl.at/FlbjK

[25] Chang, W., Arcesati, R., Hmaidi, A., *China's drive toward self-reliance in artificial intelligence: from*

chips to large language models, MERICS Report, 2025, https://shorturl.at/2ZaHv

[26] European Commission, *A Europe fit for the digital age, 2021* https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

[27] Hidary, J., Sarkar, A., *The world is heading for a 'quantum divide': here's why it matters*, 2023, https://shorturl.at/ugYho

[28] Ibrahim, A., *United States' Project Maven and the Rise Of AI-Assisted Warfare*, DefenseTalks, 2024, https://shorturl.at/xrY6P

[29] Calle, M., *Cyber Warfare in Russo-Ukrainian War*, International Relations Review, 2025, https://shorturl.at/gH4US

[30] Naprys, E., *Poland avoids blackout as PM blames Russia-linked attackers for massive cyberattack*, CyberNews, 2026, https://shorturl.at/7zsaP

[31] Neuberger, A., *China Is Still Winning the Battle for 5G—and 6G*, Foreign Affairs, 2025, https://shorturl.at/DMz4Q

[32] Defence24, *Russia's information war 2025: disinformation as an operational weapon*, 2025, https://shorturl.at/EpLFb

[33] US Senate Select Committee on Intelligence, *Bipartisan Report on Russia's Use of Social Media*, 2019, https://shorturl.at/QSpTf

[34] Martin, B., Tarraf, D., Whitmore, T., DeWeese, J., Kenney, C., Schmid, J., Paul DeLuca, P., *Advancing Autonomous Systems. An Analysis of Current and Future Technology for Unmanned Maritime Vehicles*, RAND Corporation report RR2751, 2019, https://shorturl.at/QxMan

[35] Shabbir, M., *US-China Arms Race in Space: Implications for Global Security*, RMIT University, 2025, https://shorturl.at/CbvGR

[36] Iliadis, A., Acker, A., *The seer and the seen: Surveying Palantir's surveillance platform,* The Information Society, 38(5), 334–363., 2022, DOI:0.1080/01972243.2022.2100851

[37] Pugnet, A., Strohmaier, B, Henning, M., *Palantir is well on its way to conquering Europe*, Euractiv, 2025, https://shorturl.at/VGEZt

[38] Down, A., Cole, D., *MPs question UK Palantir contracts after investigation reveals security concerns*, The Guardian, 2025, https://shorturl.at/BRX8T

Coerciția tehnologică ca instrument al politicii de stat: reconfigurarea echilibrul de putere militar global prin controlul asupra tehnologiilor emergente

Rezumat: Coerciția tehnologică (utilizarea strategică a controlului asupra tehnologiilor critice pentru a exercita influență geopolitică) redefinește raporturile de putere și puterea militară în secolul XXI. Această lucrare demonstrează că dominația în domeniul inteligenței artificiale, infrastructurii de date, sistemelor autonome și lanțurilor de aprovizionare cu semiconductori a devenit un instrument principal de coerciție, permițând statelor să proiecteze puterea fără conflict direct. Prin diverse studii de caz, lucrarea demonstrează modul în care dependența tehnologică creează un efect de levier asimetric, vulnerabilitate operațională și colonialism algoritmic. Lucrarea se încheie cu opt recomandări strategice pentru națiuni pentru a construi ecosisteme tehnologice rezistente și suverane, a impune transparența algoritmică și a reforma dreptul internațional pentru a aborda coerciția condusă de inteligența artificială.

Maria CONSTANTINESCU, Phd, Associate Professor, National Defense University Carol I, Regional Department of Defense Resources Management Studies, constantinescumaria.ro@gmail.com, +40 723 885 642, 68-72 Panduri Road, Bucharest, Romania.

Paul TUDORACHE, PhD, Professor, "Nicolae Bălcescu" Land Forces Academy, Department of Military Sciences, tudorache.paul@armyacademy.ro, +40 723 648 611, 3-5 Revolutiei Street, Sibiu, Romania.