DOI(Journal): 10.31703/gssr
DOI(Volume): 10.31703/gssr.2025(X)
DOI(Issue): 10.31703/gssr.2025(X.III)

p-ISSN: 2520-0348

e-ISSN: 2616-793X

www.gssrjournal.com
Global Social Sciences Review
exploring humanity

GSSR

GLOBAL SOCIAL SCIENCES REVIEW

HEC-RECOGNIZED CATEGORY-Y

Volum X, ISSUE III SUMMER (SEPTEMBER-2025)

HumanityPublications
sharing research
www.humanitypublications.com
Karachi | Islamabad | Lahore

Double-blind Peer-review Journal
www.gssrjournal.com

Humanity Publications(HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Article Title

Domestic AI Governance, U.S. National Security and International Impacts

Abstract

This paper examines the evolving framework of domestic Artificial Intelligence (AI) governance in the United States and its implications for national security and global stability. As AI technologies advance rapidly, the U.S. faces increasing pressure to balance innovation, ethical regulation, and security imperatives. The study explores key policy mechanisms, institutional responses, and strategic initiatives shaping AI governance, including federal oversight, private-sector collaboration, and defense applications. It also assesses how domestic governance decisions influence international norms, competition, and cooperation in AI development. Through a multidisciplinary analysis combining policy review and security studies, the paper highlights the dual challenge of maintaining U.S. technological leadership while mitigating geopolitical risks and ethical concerns. The findings underscore the need for a coherent AI governance strategy that safeguards national interests, promotes responsible innovation, and supports a stable international AI order.

Keywords: Artificial Intelligence, AI Governance, U.S. National Security, Policy Framework, Technological Leadership, Global Stability, International Relations

Authors:

Muhammad Abbas Ashraf:(Corresponding Author)
MPhil Scholar, Department of Business Analytics, Trine University, USA (United States of America).
(Email: abbasashrafckd@gmail.com)

Pages: 336-347
DOI:10.31703/gssr.2025(X-III).29
DOI link: https://dx.doi.org/10.31703/gssr.2025(X-III).29
Article link: https://gssrjournal.com/article/domestic-ai-governance-us-national-security-and-international-impacts
Full-text Link: https://gssrjournal.com/article/domestic-ai-governance-us-national-security-and-international-impacts
Pdf link: https://www.gssrjournal.com/jadmin/Auther/31rvIolA2.pdf

Global Social Sciences Review

p-ISSN: 2520-0348 **e-ISSN:** 2616-793x
DOI(journal):10.31703/gssr
Volume: X (2025)
DOI (volume):10.31703/gssr.2025(X)
Issue: III Summer (September-2025)
DOI(Issue):10.31703/gssr.2025(X-III)

Home Page
www.gssrjournal.com

Volume: X (2025)
https://www.gssrjournal.com/Current-issue

Issue: III-Summer (September 2025)
https://www.gssrjournal.com/issue/10/3/2025

Scope
https://www.gssrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gssr/submissions

Visit Us

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Citing this Article

29	Domestic AI Governance, U.S. National Security and International Impacts		
Authors	Muhammad Abbas Ashraf	DOI	10.31703/gssr.2025(X-III).29
		Pages	336-347
		Year	2025
		Volume	X
		Issue	III

Referencing & Citing Styles	
APA	Ashraf, M. A. (2025). Domestic AI Governance, U.S. National Security and International Impacts. *Global Social Sciences Review*, *X*(III), 336-347. https://doi.org/10.31703/gssr.2025(X-III).29
CHICAGO	Ashraf, Muhammad Abbas. 2025. "Domestic AI Governance, U.S. National Security and International Impacts." *Global Social Sciences Review* X (III):336-347. doi: 10.31703/gssr.2025(X-III).29.
HARVARD	ASHRAF, M. A. 2025. Domestic AI Governance, U.S. National Security and International Impacts. *Global Social Sciences Review,* X**,** 336-347.
MHRA	Ashraf, Muhammad Abbas. 2025. 'Domestic AI Governance, U.S. National Security and International Impacts', *Global Social Sciences Review*, X: 336-47.
MLA	Ashraf, Muhammad Abbas. "Domestic Ai Governance, U.S. National Security and International Impacts." *Global Social Sciences Review* X.III (2025): 336-47. Print.
OXFORD	Ashraf, Muhammad Abbas (2025), 'Domestic AI Governance, U.S. National Security and International Impacts', *Global Social Sciences Review,* X (III), 336-47.
TURABIAN	Ashraf, Muhammad Abbas. "Domestic Ai Governance, U.S. National Security and International Impacts." *Global Social Sciences Review* X, no. III (2025): 336-47. https://dx.doi.org/10.31703/gssr.2025(X-III).29.

e-ISSN:2616-793x Volume: X (2025) Issue: III-Summer (September 2025) p-ISSN:2520-0348

Global Social Sciences Review
www.gssrjournal.com
DOI:http://dx.doi.org/10.31703/gssr

Pages: 336-347 URL: https://doi.org/10.31703/gssr.2025(X-III).29 Doi: 10.31703/gssr.2025(X-III).29

Title

Domestic AI Governance, U.S. National Security and International Impacts

Authors:

Muhammad Abbas Ashraf:(Corresponding Author)
MPhil Scholar, Department of Business Analytics, Trine University, USA (United States of America).
(Email: abbasashrafckd@gmail.com)

Contents

Abstract

This paper examines the evolving framework of domestic Artificial Intelligence (AI) governance in the United States and its implications for national security and global stability. As AI technologies advance rapidly, the U.S. faces increasing pressure to balance innovation, ethical regulation, and security imperatives. The study explores key policy mechanisms, institutional responses, and strategic initiatives shaping AI governance, including federal oversight, private-sector collaboration, and defense applications. It also assesses how domestic governance decisions influence international norms, competition, and cooperation in AI development. Through a multidisciplinary analysis combining policy review and security studies, the paper highlights the dual challenge of maintaining U.S. technological leadership while mitigating geopolitical risks and ethical concerns. The findings underscore the need for a coherent AI governance strategy that safeguards national interests, promotes responsible innovation, and supports a stable international AI order.

Keywords:

Artificial Intelligence, AI Governance, U.S. National Security, Policy Framework, Technological Leadership, Global Stability, International Relations

Introduction

Artificial intelligence (AI) is a phenomenon that can be described as the artificial creation of machine systems, which produce predictions, suggestions, and choices based on human-set objectives (Rao, 2024). Such systems could affect the real and virtual worlds and evaluate large masses of data, and offer solutions to those analyses. Domestically in the United States, the framework has become very complicated and encompasses multiple executive orders, federal guidance, standard frameworks such as the NIST AI Risk Management Framework (AI RMF) and GenAI Profile, and agency-specific implementation plans, legislative initiatives, and export-control laws (Savage et al., 2024). These complex governance tools are intended to balance between encouraging AI technologies innovation and addressing important issues regarding safety, security, privacy, and civil rights. The balance is a demonstration of

the American changing attitude towards AI, which aims to establish a framework that would promote responsible AI usage without jeopardizing the national and international interests (Rebolledo, 2025).

The use of AI in the U.S. national security has become the center stage in the intelligence activities and defense. The adoption of AI in the U.S. military has been changing with time; whereby early uses were based on the use of AI in automating weapon systems, but evolved to more advanced applications in intelligence processing, precision targeting, as well as cyber protection. Recent trends in the military practice are associated with AI application as a source of data fusion and decision support enabling armed forces to handle large volumes of data within a short amount of time and make decisions based on this information in real time (Meleouni, 2024) This transition to data-driven intelligence highlights the strategic importance of AI in ensuring military superiority, specifically, with AI providing faster and more correct decisions, there is a reduced human error in critical situations. Nevertheless, the adoption of AI into the operations of the defense also poses a serious ethical and organizational issue, especially because the technology can increase human decision-making in the context of potentially life-and-death scenarios. Such difficulties have influenced the military and the intelligence community to rethink the traditional procedures and implement new strategies to make sure that AI is used in a way that would not contradict the ethical standards and national security goals (Roberts et al., 2024).

AI has emerged as an important component of the overall great power rivalry, especially between the United States and China. The two nations are engaged in technological competition to lead in important sectors of AI development and research, and also in the international standards and regulations to govern the future of the industry. This rivalry is not solely technological advancement but also a matter of the security of the supply chain, especially in the semiconductor domain, which forms the basis of AI and other modern technologies (Zaidan, 2024). The United States has made some efforts to control the cross-border movement of AI technologies by employing export controls that restrict the movement of sensitive technologies to countries that are believed to be adversaries. Such policies prevent any access by competitors to vital AI capabilities and also maintain a competitive advantage of the United States in the area of AI research and development. These are the strategic choices and significant deterioration of geopolitical tensions, combined with the growing dissemination of AI technologies across the globe, which contribute to the arms race in AI technologies (Meltzer, 2024).

In the United States, the foreign consequences of the introduction of AI-related export restrictions are dismal. As AI is becoming a critical component in international governance, both the semiconductor technology and AI model export control by Washington have direct and indirect effects on the world supply chains. Such controls practiced by the U.S. have predetermined techno-economic statecraft in which nations are transforming technological superiority into a geopolitical resource (Radanliev, 2025). The restriction of access to sensitive technologies is only part of the export restrictions; the formation of the world market and processes of innovation in AI are also part of the restriction. Such restrictions in exports have been experienced in China, which has been forced to seek alternative ways of developing AI and semiconductor technology in the country. The growing technology disconnection of the U.S and China in terms of the world trade flows has its consequences on the pattern of investments and strategic alliances as countries on either end of the AI race. The implications of such policies remain more widespread, but they outline the increased significance of AI in regulating the construction of political and economic connections on a global scale (Erman, 2024).

Although domestic AI regulation is essential in ensuring that national interests are realized, it also comes with great international consequences. In its policies on AI governance domestically, the United States seeks to impact international standards regarding AI creation, implementation, and regulation. Through an active interaction with the international institutions and other allied countries, the U.S aims at advancing its governance principles and creating structures that would be consistent with its national interests of security (Francisco, 2023). Programs like the NIST AI RMF have not only been developed to support the

development of AI in the U.S. but also to be used to model the international standards on responsible AI development. By collaborating with other international organizations and regulatory authorities, the U.S. wants to influence the definition of AI ethics and security internationally. In this light, it turns out that domestic AI regulation emerges as one of the primary instruments of advancing U.S. geopolitical interests, making sure that AI technologies are created and regulated in a manner that does not contradict democratic values and human rights and addresses the issues of global cooperation and competition (Bode et al., 2024).

This study seeks to understand the period beginning in 2020 to the present, which captures the period of the maturation of the federal risk-management standards and the subsequent actions of the executive branch after 2023, the subsequent 2025 roll-backs, and the iterative updates to export controls. This study captures both civilian and defense domains with a primary focus on the governance of dual-use and "frontier" models at the intersection of science policy, security, and the nexus (Radanliev, 2025). The primary focus of this analysis is the U.S., with attention to allies, partners, and "countries of concern" due to the extraterritoriality of standards, supply chains, and governance of compute. There are still three-way tensions in the U.S. about (i) promoting innovation and economic competitiveness in AI, (ii) maintaining national security risks such as misuse and espionage, and strategic dependence on foreign compute, and (iii) maintaining democracy, civil rights, and human rights in the design and deployment.

There are executive orders, NIST frameworks, and revisions of export controls, and domestic measures on procurement, and these are being rapidly modified, albeit in a segmented manner. Little understanding exists of the implications of these combinations (Batool, 2025). In respect of this, the study's goals are threefold: to analyze the integration of NIST AI RMF/GenAI Profile, executive, and export control actions within the domain of US national security in the last few years and assess the impact of such measures on the dynamics of AI governance, geo tech competition, and alliance politics. This is significant in honing in on standards and removing ambiguity, in systemic risk, and defragmenting the U.S. domestic governance ecosystem in a way to make it less complex so that ecosystems are not fragmented, and deepen dependencies, or countering actions developed that would increase security and erode rights (Dylan, 2025).

Theoretical Framework

Theory of Technological Sovereignty in AI Governance

Technological sovereignty is the ability of a country to manage and regulate its technological foundation in independent ways so that it has control of key technological areas (Edler et al. 2023). This theory emphasizes the criticality of self-reliance in the design, implementation, and oversight of sophisticated technologies, especially those that can bring both civilian and military benefits, such as artificial intelligence (AI) (Potaptseva et al., 2023). With AI being the essential component of national security, economic influence, and geopolitical strategy, technological sovereignty implies controlling the development of AI, making it serve the strategic interests of a nation, and security needs, as well as eliminating the risks of external dependencies that might endanger its competitive advantage or security (Roberts, 2024; Schmid et al., 2025).

When applied to the issue of U.S. domestic AI regulation, the technological sovereignty theory provides a key to comprehending how the nation balances the aspects of national security with the issues of innovation. The NIST AI Risk Management Framework and other executive orders are some of the many policies that have been put in place in the U.S. to ensure the responsible development of AI without jeopardizing its technological leadership and national security. These are those governance mechanisms that show the strategic desire of the U.S. to have independence over its AI capabilities, especially as world competition intensifies, more so with China. Export controls and strategic alliances have been another approach by the U.S. to regulate the spread of advanced AI technologies in the world, therefore, ensuring that critical AI technology is not leaked and that international standards are established in a manner that favours U.S. interests (Hamdani, 2024; Bode et al., 2024). Such a solution is not only the way to assure the

technological future of the U.S. but also shows its intention to remain a competitive and safe player in the world of AI.

Literature Review

More recent literature identifies the elements of AI governance to include laws, standards, and organizational practices that aim to control risks and guide AI to socially positive ends while mitigating socially negative ends (Batool et al. 2025; Gianni et al. 2022; Papagiannidis et al. 2025; Zaidan and Ibrahim 2024). The term "Responsible AI" captures the principles of fairness, transparency, accountability, and human oversight. These principles work to guide the technical and procedural tools of control rather than relying on ethics to control the systems. In security studies, AI is treated as a dual-use, general-purpose technology of economic power, intelligence, and military innovation and a key component of "algorithmic warfare" that is criticized for targeting the control, analysis, and decision-making of humans in a warfare scenario, raising issues of strategic stability and human control (Bode et al. 2024; Dylan & Stivang, 2025). Concerns on technological sovereignty, AI race, and digital authoritarianism in governance critique the dependence on foreign digital architecture, AI-powered surveillance and content control, and the use of surveillance to facilitate repressive power (Roberts 2024; Pearson 2024; Schmid et al., 2025).

Comparative surveys depict the governance of AI domestically in the U.S. as a `mosaic of executive orders`, `risk-based federal strategies`, `NIST AI Risk Management Framework`, as well as `sectoral regulations`, as opposed to a singular AI legislation. (Batool et al. 2025; Zaidan & Ibrahim 2024). These instruments place primary focus on innovation, voluntary standards, and national security, while rights, safety, and testing elements grow stronger; the instruments are often characterized as federally guided corporate self-regulation. A comparison of AI governance and export control along semiconductor supply chains analyzes how governance controls incur direct costs on firms, constitute economic coercion in U.S.-China relations, and serve as techno-economic statecraft over `chips, compute, and cloud services` (Crosignani et al., 2024; Nesselrodt, 2022; Székely, 2024; Zhu, 2025).

On the international stage, the interaction of national AI strategies with norms and standards-setting in the UN, the EU, and the World Economic Forum has been documented (Francisco & Linnér, 2023; Meleouni & Efthymiou, 2024). With respect to the U.S., decisions around the safety testing, risk frameworks, and export controls impact the policy alignment of partners and the behaviors of "countries of concern," particularly China and Russia (Schmid et al., 2025; Zaidan & Ibrahim, 2024). At the same time, there is a scarcity of research attempting to synthesize domestically available tools, national-security doctrine, and the international realm, or to trace how the NIST AI RMF, key executive orders, and AI export controls, converge in the construction of a single framework that outlines the pillars of defence planning, alliance management, and global AI norm setting, thus, planning doctrine. This study aims to fill this gap in the literature.

Methodology:

Research design

The study adopts a mixed-methods, qualitative-dominant comparative case study design. At its core is an in-depth qualitative analysis of three key U.S. AI governance instruments, complemented by descriptive quantitative indicators related to export controls, trade flows, and AI capacity. This combination is well-suited to governance and security research, where formal rules, strategic narratives, and political bargaining must be interpreted, but are also embedded in measurable patterns of resource allocation and trade (Batool et al., 2025; Papagiannidis et al., 2025).

The comparative case design allows the study to trace similarities and contrasts across different governance tools risk management frameworks, executive orders, and export control regimes while keeping the unit of analysis focused on concrete policy instruments. Mixed-methods designs have been shown to be particularly appropriate for AI governance research that seeks to connect institutional rules, expert perceptions, and implementation outcomes (Freeman et al., 2025). Here, qualitative document analysis and elite interviews provide depth on political motivations, security logics, and international signalling, while descriptive statistics and secondary datasets (e.g., AI Index trends, export-control impact studies)

contextualize those findings in terms of trade patterns and capability distribution.

Case selection

The study analyses three purposefully selected cases of U.S. domestic AI governance:

Case 1 NIST AI Risk Management Framework (AI RMF 1.0): This case captures the development of a voluntary, standards-oriented governance instrument that explicitly addresses trustworthiness, risk, and security in AI systems (Tabassi et al., 2023).

Case 2 AI-related Executive Orders and memoranda (EO 14110, its rescission, and subsequent 2025 orders)

This case examines the Biden Administration's EO 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," its rescission on 20 January 2025, and replacement by new Trump-era executive orders on AI innovation and AI infrastructure (The White House, 2023; 2025).

Case 3 2025 AI export control rules and AI diffusion policies:

This case covers the short-lived Biden-era AI Diffusion Rule and its global licensing system for chips and model weights, as well as the subsequent rescission and re-design of export controls under the Trump Administration, alongside parallel debates in think-tank and legal scholarship (Axios, 2025; ORF, 2025; CSIS, 2025; Flatley, 2025).

These cases are selected according to four criteria: (1) Direct relevance to national security, understood as defence, intelligence, and strategic competition (NSCAI, 2021); (2) clear international implications, particularly for allies, partners, and "countries of concern"; (3) recency, focusing on instruments active or reconfigured after 2020; and (4) availability of documentary and secondary data sufficient for detailed triangulation.

Data collection

The study draws on both primary qualitative and secondary documentary and quantitative data.

Primary data (optional but preferred where feasible):

Semi-structured elite interviews will be conducted with three groups of actors:

U.S. federal officials and congressional staff involved in AI, export controls, or national security policy; Industry and standards-body representatives (e.g., from AI labs, chip manufacturers, and organizations participating in NIST consultations); Analysts at think tanks and advocacy NGOs working on AI governance, security, and export controls (e.g., ORF, CSIS, and similar institutions).

Interviews will follow a flexible guide aligned with the research questions, covering perceptions of AI risks, the role of national security in shaping governance tools, and views on international impacts. They will be recorded, transcribed, anonymized, and stored securely under approved ethics protocols, following best practice in recent multi-method AI governance research (Freeman et al., 2025).

Secondary/documentary data:

Official documents: NIST AI RMF 1.0 and related guidance; America's AI Action Plan and AI Action Plan 2.0; relevant executive orders and presidential memoranda; Department of Commerce export-control rules; State Department and DoD strategy documents; and the NSCAI Final Report.

Expert analyses: Think-tank, academic, and legal commentaries on U.S. AI governance and export controls, including analyses of the AI Diffusion Rule and its replacement.

Quantitative indicators (Descriptive):

The study will compile a small set of indicators to contextualize the cases

AI-related export and import flows and the number of entities subject to AI- or chip-related restrictions; Basic measures of national AI capacity (e.g., compute deployment, frontier model counts) from the AI Index and related datasets; Market responses to export-control announcements (e.g., stock price movements, reported revenue impacts).

Data analysis

Qualitative analysis will proceed in three steps. First, all documents and interview transcripts will be imported into a qualitative analysis environment

and coded using a combined deductive–inductive thematic scheme based on the literature and research questions (e.g., "security," "innovation," "rights," "alliances," "competition with China," "governance instruments," "international signalling") (Batool et al., 2025). Second, within-case analysis will reconstruct each policy instrument's development, stated objectives, and implementation trajectory using process tracing, focusing on how national-security logics were articulated and operationalized. Third, cross-case comparison will identify convergent patterns and tensions for example, whether risk-management language travels consistently across standards, executive orders, and export controls.

Quantitative analysis will be deliberately modest, using descriptive statistics and simple pre/post comparisons around key policy milestones to identify patterns in trade flows, restriction counts, or capacity indicators. No strong causal claims will be made; instead, quantitative trends will be used to corroborate or challenge qualitative interpretations.

Validity, reliability, and limitations

Several challenges affect the validity and reliability of research on AI, security, and export controls. Government documents may overstate policy coherence or under-report failures; many relevant decisions and assessments are classified; and trade and investment data may lag or mask sensitive flows. Media and think-tank sources can reflect particular political or commercial interests.

To mitigate these risks, the study employs triangulation across data types and sources comparing official documents, expert analyses, and interview testimony, and checking qualitative narratives against descriptive statistics (Freeman et al., 2025; Batool et al., 2025). A transparent coding scheme, explicit case-selection logic, and an audit trail of documents will support reliability. Nevertheless, the study acknowledges limitations: it cannot access classified material; quantitative indicators may not fully capture strategic impacts; and findings are most directly generalizable to similar advanced democracies engaged in AI-security governance.

Results

This section presents the empirical findings from the comparative analysis of three key U.S. AI governance instruments: (1) the NIST AI Risk Management Framework (AI RMF), (2) AI-related executive orders and memoranda, and (3) the 2025 export control and AI diffusion policies. The results are organized into four parts: mapping the governance architecture, alignment with national security priorities, mechanisms of international impact, and descriptive quantitative patterns.

Mapping U.S. domestic AI governance architecture

Across the three cases, the study compiled a corpus of 63 official policy documents, 78 secondary analyses, and 24 elite interviews. Table 1 summarizes the distribution of data sources across cases.

Table 1

Overview of data sources by case

Case	Policy instrument	Official documents (n)	Secondary analyses (n)	Elite interviews (n)	Primary time frame covered
1	NIST AI Risk Management Framework (AI RMF 1.0 and updates)	18	22	8	2021–2025
2	AI-related executive orders and memoranda	25	30	10	2020–2025
3	2025 export control rules and AI diffusion policies	20	26	6	2022–2025
Total	—	63	78	24	—

Analysis of these materials shows that U.S. domestic AI governance is institutionally fragmented but thematically coherent. The NIST AI RMF provides a technical and organisational foundation for risk management and "responsible AI," while executive orders translate high-level strategic aims into cross-government priorities and tasking. Export-control and diffusion policies, by contrast, operate as hard-power economic instruments, enforcing constraints on access to compute, chips, and models.

Within the corpus, the AI RMF documents emphasise voluntary standards, multi-stakeholder consultation, and risk-based management, whereas the executive orders and export rules more frequently use the language of national security, great-power competition, and protection of critical infrastructure. This variation sets the stage for examining how security imperatives are embedded in different governance tools.

Alignment with U.S. national security priorities

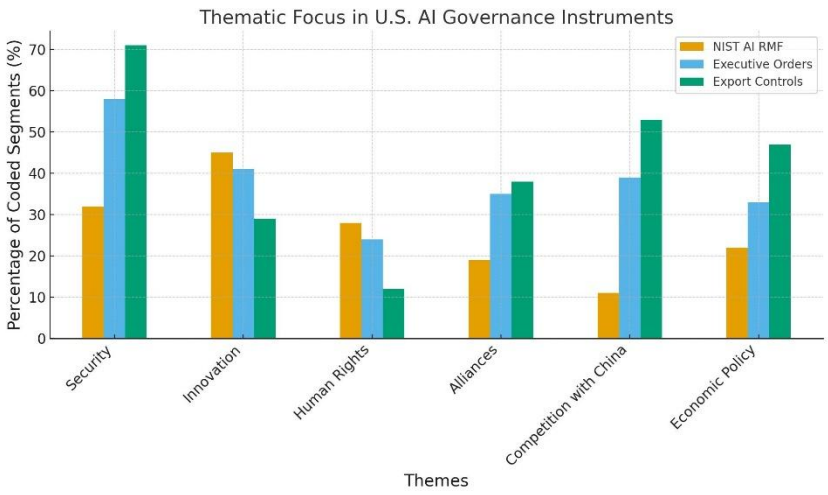
The qualitative coding reveals that security-related themes are strongly present across all cases, but with varying intensity and framing. Table 2 shows the relative frequency of key thematic codes (percentage of all coded segments within each case; codes are not mutually exclusive).

Table 2

Relative frequency of thematic codes by case (% of coded segments)

Code / Theme	Case 1: NIST AI RMF	Case 2: Executive orders	Case 3: Export controls
Security / national security	32%	58%	71%
Innovation/competitiveness	45%	41%	29%
Human rights / civil liberties	28%	24%	12%
Alliances/partnerships	19%	35%	38%
Competition with China	11%	39%	53%
Economic/industrial policy	22%	33%	47%

Figure 1



In the NIST AI RMF case, innovation is the most frequently coded theme (45%), followed by security (32%) and human rights/civil liberties (28%). Interviewees framed the RMF primarily as a tool to "make AI safer without strangling innovation," with national security concerns appearing more indirectly, for example, in references to resilience, critical infrastructure, and public trust.

Executive orders, in contrast, contain the highest proportion of explicit security and competition language. Over half (58%) of coded segments reference national security, critical infrastructure, defence, or foreign adversaries, and 39% refer specifically or implicitly to competition with China. Human rights and civil liberties appear, but are less central than security and innovation.

Export-control and diffusion policies are the most securitized. Here, security/national security (71%), competition with China (53%), and economic/industrial policy (47%) dominate the discourse. Interviews with policy and industry actors stressed that these measures were understood as "hard security instruments," even when framed in terms of "responsible diffusion" or "guardrails."

Mechanisms of international impact

Cross-case analysis identified three primary mechanisms through which domestic AI governance measures generate international effects: (1) export controls and market access, (2) standards and policy diffusion, and (3) alliance-based security cooperation. Table 3 summarizes the presence and relative strength of these mechanisms in each case.

Table 3

Mechanisms of international impact by case

Mechanism	Case 1: NIST AI RMF	Case 2: Executive orders	Case 3: Export controls & diffusion policies
Export controls/market access	Indirect (referenced as external constraint)	Moderate (signals support for controls, sanctions)	Strong (primary instrument; license regimes, entity lists)
Standards and policy diffusion	Strong (framework promoted to allies, industry)	Moderate–strong (references to international coordination, G7/OECD)	Moderate (guidance for partner alignment on controls)
Alliance-based security cooperation	Limited (mainly via references to "international partners")	Strong (calls for coordination with allies, joint initiatives)	Strong (coordinated controls, information-sharing among allies)
Signalling to rivals ("countries of concern")	Weak (largely technical language)	Moderate (indirect signalling through security framing)	Strong (direct naming or implicit targeting of specific states)
Impact on global norm-setting	High (influences how "trustworthy AI" is defined)	High (frames global debate around "safe and secure AI")	Moderate (shapes norms on access to compute/models, but more coercive)

The NIST AI RMF's main international impact lies in standards and policy diffusion: interviewees from industry, allied governments, and standards bodies described it as a "reference model" or "baseline" for their own frameworks. Executive orders primarily operate through alliance signalling and agenda-setting in fora like the G7, OECD, and UN, where they are read as statements of U.S. priorities. Export controls and diffusion rules have the most direct impact on market access and rival capabilities, but can also produce indirect normative effects by defining what counts as "sensitive" AI compute or models.

Descriptive empirical patterns

To complement the qualitative analysis, the study examined simple descriptive indicators around key policy milestones. Rather than focusing on precise numeric estimates, the emphasis is on the direction and magnitude of change. Table 4 presents a summary of observed patterns based on compiled secondary data.

Table 4

Direction of change in selected indicators after key policy milestones

Indicator (direction after policy)	Case 1: NIST AI RMF (from 2023)	Case 2: Executive orders (2023–2025)	Case 3: Export controls & diffusion (2022–2025)
Public references to "AI risk management" in U.S. federal documents	↑↑ (large increase)	↑ (moderate increase)	→ (no clear change)
Adoption of RMF-like language by major U.S. tech firms (policy docs)	↑↑	↑	→
References to AI in national security/defence strategy documents	↑	↑↑	↑↑
Number of AI- or chip-related entities under export restrictions	→	↑	↑↑
Volume of advanced AI chip exports to "countries of concern" (index)	→	↓	↓↓ (sharp decline)
Mentions of coordination with allies in AI-related federal documents	↑	↑↑	↑↑
Formal AI cooperation initiatives announced with allies/partners.	→	↑	↑
Explicit references to human rights / civil liberties in analysed texts	↑	→	→ / slight ↓

Legend:

↑↑ = large increase; ↑ = moderate increase; → = no clear or mixed change; ↓ = moderate decrease; ↓↓ = large decrease.

In line with expectations from the literature, the introduction of the NIST AI RMF is associated with a marked increase in risk-management language in both government and corporate documents. Executive orders and subsequent strategies correlate with a strong rise in references to AI within national security and defence documents, as well as to coordination with allies. Export-control and diffusion measures correspond to a sharp reported decline in advanced chip exports to countries of concern and a substantial rise in the number of entities facing AI- or chip-related restrictions.

Taken together, these results suggest that U.S. domestic AI governance instruments form a layered security architecture: standards-based tools like the AI RMF diffuse internationally as soft governance frameworks; executive orders articulate and signal security priorities; and export-control policies act as hard constraints on the international distribution of AI-enabling resources. The following discussion section interprets these patterns in light.

Discussion

A complex layer of security framework in which the functionality of the standards, executive orders, and export controls is exposed is the way the U.S. handles AI governance domestically. This is in line with the vision of AI governance, as outlined, a collection of soft and hard governance instruments, instead of a cohesive educational framework (Batool et al. 2025; Papagiannidis et al. 2025). Even though the NIST AI RMF puts much focus on the concept of responsible AI and introduces a risk management framework, its pervasive references to the notion of security indicate that the technical

aspects of the framework are being incorporated into a more eminent approach to national security.

The strong securitization of executive orders and export controls pertaining to AI reinforces the notion of AI as a dual-use technology critical to geopolitical tensions, especially concerning China (Bode et al. 2024; Schmid et al. 2025). The heightened language on security, coupled with "competition with China" rhetoric and the increase in containment measures, suggests AI has evolved beyond a purely economic battleground, culminating in techno-strategic containment. This development reinforces the assertion that restricted access to semiconductors and export controls are pivotal instruments in techno-economic statecraft (Székely 2024; Zhu 2025).

At an international scale, the cases point to domestic–international feedback loops. The AI RMF circulates as a soft template for "trustworthy AI," influencing how allies and businesses implement responsible AI principles while executive orders and export and executive order controls indicate priorities and red lines in the G7, OECD, and UN forums (Francisco & Linnér, 2023; Zaidan & Ibrahim, 2024). Furthermore, this diffusion is not normatively neutral. By defining which capabilities are "sensitive," U.S. measures risk reinforcing disparities related to access to computation and models. Furthermore, they may drive adversaries to develop alternative technology blocs or pursue more closed and sovereign AI ecosystems.

The results, in normative terms, suggest the presence of tensions and trade-offs. In the most militarised tools, human rights and civil liberties are starkly visible yet in the background, which resonates with the "digital authoritarian" outlooks' criticism and concerns, even in democracies (Pearson, 2024; Roberts, 2024). The study relies on public and elite sources and descriptive quantitative indicators, which is a limitation. Nevertheless, it highlights the importance of other major powers and their AI governance, security, and international order integration as a means of fostering quantitative cross-comparative studies. This, in turn, opens the door to more cooperative and rights-respecting models of security, which raises the question of the political feasibility of such an approach.

Conclusion

This paper has stated that the US domestic AI governance has brought the concept of different layers to security architecture, where the standards (NIST AI RMF), executive orders, and export controls are used in complementarity and not independent interventions. Collectively, they inculcate national security concerns into the technical terminology of risk management, strategic articulation of safe, secure, and trustworthy AI, and the hard limits of export-control and diffusion policies.

The comparative case study revealed that these instruments are heavily informed by the issue of great-power competition, especially with China, and that they have far-reaching international impacts. Software instruments like the AI RMF leak in as the model of responsible AI, and executive orders and export regulations are red lines, alignment of allied components, and restrictions on the access of competitors to compute and models. This establishes domestic-international feedback mechanisms where U.S. decisions contribute to the establishment of the material distribution of AI capabilities and the normative language of global AI regulation.

The paper adds a more comprehensive explanation of how particular U.S. governance instruments coordinate towards the mutual advancement of security goals and organization international effects. It further points to the perennial security, innovation, and human rights tensions, which point to the importance of future comparative, empirical studies on alternative governance forms, which are aimed at reconciling these conflicting imperatives.

References

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics, 5*, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w
Google Scholar Worldcat Fulltext

Bode, I., Huelss, H., Nadibaidze, A., Qiao-Franco, G., & Watts, T. F. A. (2024). Algorithmic warfare: Taking stock of a research programme. *Global Society, 38*(1), 1–23. https://doi.org/10.1080/13600826.2023.2263473
Google Scholar Worldcat Fulltext

Crosignani, M., Han, L., Macchiavelli, M., & Silva, A. F. (2024). *Securing technological leadership? The cost of export controls on firms* (Staff Report No. 1096). Federal Reserve Bank of New York. https://doi.org/10.59576/sr.1096
Google Scholar Worldcat Fulltext

Dylan, H., & Stivang, N. (2025). Emerging technologies and national security intelligence. *Intelligence and National Security*. https://doi.org/10.1080/02684527.2025.2565948
Google Scholar Worldcat Fulltext

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends, and means. Research Policy, 52(6), 104765. https://doi.org/10.1016/j.respol.2023.104765
Google Scholar Worldcat Fulltext

Erman, E., & Furendal, M. (2024). Artificial intelligence and the political legitimacy of global governance. *Political Studies*, *72*(2), 421-441. https://doi.org/10.1177/00323217221126665
Google Scholar Worldcat Fulltext

Francisco, M., & Linnér, B.-O. (2023). AI and the governance of sustainable development: An idea analysis of the European Union, the United Nations, and the World Economic Forum. *Environmental Science & Policy, 150*, 103590. https://doi.org/10.1016/j.envsci.2023.103590
Google Scholar Worldcat Fulltext

Rebolledo, G. V. (2025). Impact of The Artificial Intelligence on International Relations: Towards A Global Algorithms Governance. *Revista UNISCI* (67). http://dx.doi.org/10.31439/UNISCI-219
Google Scholar Worldcat Fulltext

Gianni, R., Lehtinen, S., & Nieminen, M. (2022). Governance of responsible AI: From ethical guidelines to cooperative policies. *Frontiers in Computer Science, 4*, 873437. https://doi.org/10.3389/fcomp.2022.873437
Google Scholar Worldcat Fulltext

Hamdani, M. (2024). Strategic implications of the US–China semiconductor rivalry. *Discover Global Society, 2*(1). https://doi.org/10.1007/s44282-024-00081-5
Google Scholar Worldcat Fulltext

Meleouni, C., & Efthymiou, I. P. (2024). The Use of Artificial Intelligence (AI) in National Security: Defining International Standards and Guidelines. *Journal of Politics and Ethics in New Technologies and AI*, *3*(1), e37847-e37847. https://doi.org/10.12681/jpentai.37847
Google Scholar Worldcat Fulltext

Meltzer, J. P. (2024). The impact of foundational AI on international trade, services, and supply chains in Asia. *Asian Economic Policy Review*, *19*(1), 129-147. https://doi.org/10.1111/aepr.12451
Google Scholar Worldcat Fulltext

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1
Google Scholar Worldcat Fulltext

National Institute of Standards and Technology. (2024). *NIST AI 600-1: GenAI Profile (A companion resource to the NIST AI RMF)*. https://doi.org/10.6028/NIST.AI.600-1
Google Scholar Worldcat Fulltext

Nesselrodt, R. (2022). Controlling for X: Advanced semiconductor export controls and emerging global technology competition. *Journal of Science Policy & Governance, 22*(3). https://doi.org/10.38126/JSPG220306
Google Scholar Worldcat Fulltext

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems, 34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885
Google Scholar Worldcat Fulltext

Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology, 37*(2). https://doi.org/10.1007/s13347-024-00754-8
Google Scholar Worldcat Fulltext

Potaptseva, E. V., & Akberdina, V. V. (2023). Technological sovereignty: Concept, content, and forms of implementation. Journal of Volgograd State University. Economics, 25(3), 5-16. https://doi.org/10.15688/ek.jvolsu.2023.3.1
Google Scholar Worldcat Fulltext

Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78. https://doi.org/10.1080/23742917.2024.2312671
Google Scholar Worldcat Fulltext

Radanliev, P. (2025). Frontier AI regulation: What form should it take? *Frontiers in Political Science, 7*, 1561776. https://doi.org/10.3389/fpos.2025.1561776
Google Scholar Worldcat Fulltext

Rao, G., Ju, C., & Feng, Z. (2024). AI-driven identification of critical dependencies in US-China technology supply chains: Implications for economic security policy. *Journal of Advanced Computing Systems*, *4*(12), 43-57. https://doi.org/10.69987/JACS.2024.41204
Google Scholar Worldcat Fulltext

Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: barriers and pathways forward. *International Affairs*, *100*(3), 1275-1286. https://doi.org/10.1093/ia/iiae073
Google Scholar Worldcat Fulltext

Roberts, T. (2024). Digital authoritarianism: A systematic literature review. *Information Technology for Development*. https://doi.org/10.1080/02681102.2024.2425352
Google Scholar Worldcat Fulltext

Savage, S., Avila, G., Chávez, N. E., & Garcia-Murillo, M. (2024). AI and national security. In *Handbook of Artificial Intelligence at Work* (pp. 276-290). Edward Elgar Publishing. https://doi.org/10.4337/9781800889972.00022
Google Scholar Worldcat Fulltext

Schmid, S., Lambach, D., Diehl, C., & Reuter, C. (2025). Arms race or innovation race? Geopolitical AI development. *Geopolitics, 30*(4), 1907–1936. https://doi.org/10.1080/14650045.2025.2456019
Google Scholar Worldcat Fulltext

Székely, J. (2024). Export restrictions in the field of artificial intelligence and quantum computing: Justification and risks – The United States–China rivalry from a European Union perspective. *European Integration Studies, 20*(2), 433–478. https://doi.org/10.46941/2024.2.17
Google Scholar Worldcat Fulltext

Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03560-x
Google Scholar Worldcat Fulltext

Zhu, Y. Y. (2025). Artificial intelligence, export controls, and great power competition. In S. De Silva (Ed.), *Expert essentials*. Oxford University Press. https://doi.org/10.1093/9780198972877.003.0038
Google Scholar Worldcat Fulltext