The Cyber Governance Trilemma: Comparative AI Regulation in the EU, China, and the United States

Jon Chun[1]

Christian Schroeder de Witt[2]

Katherine Elkins[1]

[1]Kenyon College

[2]University of Oxford

Abstract

Artificial intelligence regulation has emerged as a defining challenge for international cyber governance. As AI systems become deeply embedded in critical infrastructure, cybersecurity operations, and information ecosystems, the frameworks governing their development and deployment increasingly shape the global cyber policy landscape. This paper presents a comparative analysis of the three most influential AI regulatory approaches: the EU AI Act, China's sector-specific regulations, and the US approach spanning Executive Order #14110, its revocation under the Trump administration, and state-level initiatives including California's SB 53. Drawing on regulatory competition theory, a governance typology grounded in comparative regulatory capitalism, and the concept of regime complexity, we argue that these three jurisdictions face a *cyber governance trilemma*: no jurisdiction can simultaneously optimise innovation speed, safety and rights protection, and regulatory interoperability. The EU prioritises safety at the cost of innovation velocity; the US prioritises innovation at the cost of consistent safety guarantees; China prioritises state-directed competitiveness at the cost of international interoperability. This regulatory fragmentation is itself a cyber risk, creating compliance gaps that sophisticated threat actors can exploit and complicating international norm-building processes. Incorporating developments through late 2025, we conclude with implications for international cyber governance, including lessons for developing nations navigating between competing regulatory models.

Keywords: AI regulation, cyber governance, regulatory fragmentation, EU AI Act, comparative policy, Brussels Effect

1 Introduction

The regulation of artificial intelligence has become inseparable from cyber governance. AI-generated deepfakes now undermine election integrity and enable sophisticated social engineering attacks; autonomous agents probe critical infrastructure for vulnerabilities at machine speed; and adversarial actors exploit large language models to generate polymorphic malware that evades signature-based defences.[1] At the same time, AI systems have become indispensable to cyber defence, powering anomaly detection in financial networks, automating threat intelligence, and orchestrating incident response across complex digital ecosystems. The frameworks that govern AI development and deployment therefore shape the cyber threat landscape directly: how a jurisdiction regulates AI determines not only the safety of its own digital infrastructure but the security posture of every interconnected system.[2]

As jurisdictions race to regulate these dual-use capabilities, the resulting patchwork of divergent frameworks creates a new form of systemic cyber risk: regulatory fragmentation. Where cybersecurity once centred on technical standards and incident response, the governance challenge has expanded to encompass the foundational question of how societies choose to develop, deploy, and constrain AI.[3] The divergent answers emerging from the EU, China, and the United States carry direct implications for domestic technology policy and for the architecture of international cyber governance. Gaps between regulatory regimes create seams that sophisticated threat actors can exploit: an AI system that satisfies Chinese content-labelling requirements may violate EU transparency standards, while a system compliant with the EU AI Act's high-risk provisions may be entirely unregulated under the post-2025 US framework.

A growing body of scholarship has examined how different jurisdictions are approaching AI governance. Early comparative work mapped the ethical principles underpinning national AI strategies in the US, EU, and UK,[45] while Stix identified three distinct policy pathways (ethics-based, rights-based, and risk-based) that governments have pursued.[6] Smuha documented the emergence of 'regulatory competition' in AI, arguing that jurisdictions are now racing not only to develop AI but to set the rules governing it.[7] Studies have examined individual regimes in depth, including the EU AI Act,[8] China's layered regulatory approach,[9] and the broader framing contests that shape AI policy.[10] However, few studies offer a systematic three-way comparison that situates the EU, China, and the US within a unified analytical framework or examines AI regulation through the lens of cyber governance: a gap this paper seeks to address.

The regulatory landscape has shifted dramatically since 2024. The EU AI Act's prohibitions on high-risk AI practices took effect in February 2025. In the United States, President Trump revoked Executive Order #14110 on his first day in office in January 2025, while California enacted a successor transparency law (SB 53) in September 2025 and New York passed the RAISE Act in December 2025. China amended its Cybersecurity Law in October 2025 to incorporate AI governance provisions for the first time in national legislation. AI regulation is evolving rapidly and unevenly across jurisdictions, with direct consequences for the coherence of international cyber governance.

The paper contributes in three ways. It provides a systematic comparative analysis of AI regulatory frameworks across the three major AI economies, updated through late 2025. It introduces a *cyber governance trilemma*, the proposition that jurisdictions cannot simultaneously optimise innovation speed, safety and rights protection, and regulatory interoperability, and shows how each jurisdiction resolves this trilemma differently. And it draws out implications for international cyber governance, including for developing nations caught between competing regulatory models.

2 Theoretical Framework

Comparative studies of technology regulation have long observed that jurisdictions adopt divergent governance strategies shaped by institutional traditions, political economy, and geopolitical positioning.[11][12] As Smuha argues, the global 'race to AI regulation' now rivals the race to develop the technology itself.[13] This paper draws on four complementary theoretical perspectives to move beyond description towards analytical comparison.

First, we draw on *regulatory competition theory*, which holds that jurisdictions compete, and learn from one another, through their regulatory choices.[14] Bradford's concept of the 'Brussels Effect' describes a mechanism by which the EU's large single market incentivises global firms to adopt EU standards unilaterally. We examine whether the EU AI Act exhibits this dynamic and how competing regulatory models may limit it.

Second, we employ a *governance typology* that distinguishes regulatory frameworks along two dimensions: (1) the degree of *centralisation* (top-down versus distributed) and (2) the primary *regulatory modality* (ex ante risk-based rules versus ex post enforcement through existing legal frameworks). This typology draws on Majone's analysis of the 'regulatory state' in Europe[15] and Levi-Faur's account of the 'global diffusion of regulatory capitalism',[16] applying their comparative frameworks to the AI domain. The typology reveals that the three jurisdictions occupy distinct positions: the EU favours centralised, ex ante regulation; the US favours distributed, ex post enforcement; and China occupies a hybrid position combining centralised guidance with decentralised, sector-specific implementation.

Third, we attend to the *innovation–safety tradeoff* that pervades AI governance debates globally.[17] Each jurisdiction resolves this tension differently, reflecting deeper differences in political values: the EU privileges precaution and fundamental rights,[18] China prioritises social stability alongside state-directed industrial competitiveness,[19] and the US emphasises market-driven innovation with voluntary commitments.

Fourth, we draw on Nye's concept of *regime complexity*[20] and the broader literature on internet governance fragmentation[21][22] to situate AI regulation within the evolving architecture of cyber governance. The absence of a single overarching regime for AI governance, mirroring the fragmented regime complex that characterises cyberspace more broadly, has direct implications for international cooperation, norm-building, and the management of transboundary cyber risks.[23]

3 Methodology

This study employs a comparative case study methodology to examine how AI regulatory frameworks interact with, and reshape, the cyber governance landscape across three jurisdictions: the European Union, the People's Republic of China, and the United States (at both federal and state levels). Case selection follows a most-different-systems design: the three cases represent the world's largest AI economies while instantiating distinct governance traditions: centralised ex ante regulation, hybrid state-guided governance, and distributed market-oriented oversight. This design allows identification of structural factors that drive regulatory divergence and its cyber governance consequences.

Our analytical approach combines *legal and policy document analysis* with *regime complexity mapping*. For each jurisdiction, we examined the principal legislative texts, executive orders, regulatory guidance, and enforcement actions current through late 2025, with particular attention to provisions governing AI systems in cybersecurity-relevant domains: critical infrastructure, defence and intelligence, surveillance, and information integrity. We supplement primary legal sources with peer-reviewed scholarship, policy institute reports, and practitioner commentary. The comparison is structured around the governance typology and regime complexity frameworks introduced above, with the comparative regulatory timeline (Section 4) serving as an original empirical anchor for tracking the pace, sequencing, and competitive dynamics of regulatory activity across jurisdictions.

4 Comparative Regulatory Timeline

Table 1 presents a comparative regulatory timeline constructed as a structured dataset of AI governance milestones across the three jurisdictions. Inclusion criteria were: (1) binding legislation, executive orders, or regulations with direct AI governance provisions; (2) institutional actions establishing new AI-specific governance bodies; and (3) enforcement milestones marking the operational commencement of regulatory obligations. Non-binding strategies, voluntary commitments, and subnational actions below the state or provincial level were excluded unless they demonstrably shaped national regulatory trajectories (as California's SB 1047 debate did for US AI governance).

Date	**Jurisdiction**	**Milestone**
Nov 2016	China	Cybersecurity Law adopted (effective June 2017)
Apr 2018	EU	AI Strategy: *Artificial Intelligence for Europe*
Feb 2019	US	Executive Order 13859 on maintaining US leadership in AI
Apr 2021	EU	AI Act proposed by European Commission
Sept 2021	China	Data Security Law takes effect
Nov 2021	China	Personal Information Protection Law (PIPL) takes effect
Mar 2022	China	Algorithm Recommendation Regulation takes effect
Oct 2022	US	Blueprint for an AI Bill of Rights
Jan 2023	China	Deep Synthesis Regulation takes effect
Aug 2023	China	Generative AI Measures take effect
Oct 2023	US	Biden signs EO #14110 (100+ delegated tasks to 50+ agencies)
Dec 2023	EU	AI Act provisionally agreed (European Parliament + Council)
Jan 2024	US	NIST establishes US AI Safety Institute
Aug 2024	EU	AI Act enters into force
Sept 2024	US	Governor Newsom vetoes California SB 1047
Jan 2025	US	Trump revokes EO #14110; signs EO 14179 (3 days later)
Feb 2025	EU	Prohibited AI practices take effect
Aug 2025	EU	GPAI model governance obligations take effect
Aug 2025	China	State Council issues 'AI Plus' Action Plan
Sept 2025	US	California enacts SB 53 (Transparency in Frontier AI Act)
Oct 2025	China	NPC amends Cybersecurity Law to incorporate AI governance
Dec 2025	US	New York enacts RAISE Act
Aug 2026	EU	High-risk AI system requirements take effect (scheduled)

Table 1: Comparative timeline of major AI regulatory milestones (2016–2026).

Several patterns emerge from the timeline. First, the data reveal a clear acceleration: only three entries fall before 2021, while fifteen fall between 2023 and 2026, reflecting the post-ChatGPT urgency that swept all three jurisdictions simultaneously. Second, the jurisdictions exhibit distinct sequencing strategies. China led with targeted, sector-specific regulations (algorithmic recommendation, deepfakes, generative AI) before attempting consolidation through Cybersecurity Law amendments in 2025. The EU pursued a single comprehensive legislative instrument over a multi-year process, accepting slower adoption in exchange for systemic coherence. The US oscillated between executive action and state-level experimentation, with the revocation of EO #14110 representing a dramatic reversal in federal-level ambition. Third, the timeline reveals periods of competitive acceleration, notably the 2023–2025 cluster in which all three jurisdictions undertook major regulatory actions within months of each other, suggesting the regulatory competition dynamics that Smuha theorised.[24] For cyber governance, the acceleration pattern is consequential: rapid, uncoordinated regulatory proliferation across jurisdictions compounds the interoperability challenges that the trilemma describes.

5 The European Union

5.1 Overview

The 2024 EU AI Act is positioned as the world's first comprehensive AI law.[25] Just as prior European general-purpose legislation, such as the 2016 General Data Protection Regulation (GDPR),[26] the EU AI Act represents complex joint efforts across various EU bodies, including the European Commission, the European Parliament, and the European Council. Influence on the Act's formation was taken publicly by national government officials, such as France's Macron lobbying for exemptions for open-source AI providers such as Mistral,[27] as well as by lobbying and industry groups, including Big Tech[28] and German pro-open-source non-profit LAION.[29]

The Act was first constructed within a product safety framework, but then blended with a fundamental rights agenda at the behest of the European Parliament.[30] This approach resulted in a unique syncretism, clearly setting the EU AI Act apart from prior legislation building on established frameworks such as the GDPR. The Act also follows earlier European regulatory initiatives, including the 2022 Digital Markets Act[31] and, of direct relevance to cyber governance, the NIS2 Directive on cybersecurity.[32] The interaction between the AI Act and NIS2 creates the most integrated AI-cybersecurity governance framework among the three jurisdictions examined here. The NIS2 Directive, which entered into force in January 2023 and required member-state transposition by October 2024, designates operators in energy, transport, banking, health, digital infrastructure, and public administration as 'essential entities' subject to mandatory cybersecurity risk management and incident reporting. Where AI systems are deployed within these sectors (as they increasingly are, for grid management, fraud detection, medical diagnostics, and network traffic analysis) providers must satisfy both the AI Act's risk-based requirements and NIS2's cybersecurity obligations simultaneously. This regulatory overlap is deliberate: it reflects the EU's systemic approach to digital governance, in which AI safety, data protection (GDPR), and cybersecurity (NIS2) form an interlocking regulatory architecture.

5.2 The Geopolitics of the Act

Besides regulating the EU single market, the Act is widely regarded as a strategic effort by the European Commission to establish themselves as the leading AI rulemakers globally.[33] It is speculated that companies across the world will begin to prioritise compliance with European AI law out of economic necessity, not through coercion: the 'Brussels Effect'.[34][35] One direct institutional consequence is the establishment of the EU AI Office, which will oversee AI regulation, provide a central pool of AI expertise to member states, and support a 'strategic, coherent, and effective European approach on AI at the international level'.[36]

5.3 Risk Classification and Regulation

The Act is designed as an *adaptive legislation*, with details intentionally left open for later specification. At its core lies a risk classification system that places obligations primarily on the developers ('providers') of AI systems. The Act applies not only to systems placed on the market within the EU, but also to AI systems whose output is used in the EU, giving the Act considerable extraterritorial reach.

The Act defines four risk tiers. *Prohibited practices* include AI systems used for social scoring, manipulative subliminal techniques, and most real-time remote biometric identification.[37] *High-risk systems* constitute the majority of regulation, requiring risk management systems, data governance, human oversight, and cybersecurity measures.[38] *Limited-risk* systems face transparency obligations, while *minimal-risk* systems are left unregulated.

For cyber governance, the high-risk category matters most. AI systems used as safety components of critical infrastructure (Annex III, Area 2), AI systems used for law enforcement and border control (Annex III, Areas 6–7), and AI systems deployed in democratic processes all fall within this tier. Article 15 of the Act explicitly requires providers of high-risk AI systems to achieve an 'appropriate level of cybersecurity' proportionate to the risks, including resilience against adversarial manipulation, data poisoning, and model extraction attacks, requirements that mirror and reinforce NIS2 obligations for essential entities. This is the clearest example in any jurisdiction of AI regulation being explicitly linked to cybersecurity standards.

Among models, the Act further distinguishes *general-purpose AI (GPAI) models*, with heightened obligations for those posing 'systemic risk', defined as models trained with cumulative compute exceeding 10^{25} floating-point operations.[39] Providers must register with the European Commission and adhere to wide-ranging safety and security criteria, including adversarial testing and model evaluation.

5.4 Open Source and Innovation

The Act contains wide-ranging exemptions for providers of AI systems under free and open-source software licences,[40] provided they do not contain GPAI models of systemic risk. However, the partial nature of these exemptions, narrower than the de facto permissive environment in both the US and China, remains a critical unresolved tension.

5.5 Implementation Progress (2025)

By late 2025, the AI Act had moved from legislative ambition to operational enforcement. The prohibited-practices provisions, banning social scoring, manipulative subliminal techniques, and most real-time remote biometric identification, became legally binding on 2 February 2025. GPAI model governance obligations followed on 2 August 2025, with penalties reaching €35 million or 7% of global annual turnover for non-compliance. Full high-risk AI system requirements are scheduled for August 2026. In parallel, NIS2 transposition deadlines drove member states to integrate AI-specific cybersecurity obligations into national frameworks, creating a synchronised rollout of AI safety and cybersecurity governance unprecedented among the three jurisdictions.

6 China

6.1 Overview

China's approach to AI governance occupies a distinctive hybrid position: centralised strategic direction combined with decentralised, sector-specific implementation and selective enforcement. The central government sets overarching objectives (social stability, technological self-sufficiency, and 'core socialist values') while provincial governments and sectoral regulators translate these into operational rules, often with considerable latitude for local experimentation.[41] The design is a deliberate attempt to take the best of both the EU model (coherent top-down guidance) and the US model (market-driven innovation) while avoiding the perceived weaknesses of each.

What sets China apart from a cyber governance perspective is its institutional architecture. The Cyberspace Administration of China (CAC) is simultaneously the country's internet regulator, data protection authority, and primary AI governance body. This consolidation is deliberate: it ensures that AI regulation operates within, and reinforces, China's broader cyber sovereignty strategy, in which data governance, content control, algorithmic regulation, and cybersecurity are a single governance ecosystem rather than separate policy domains.

6.2 Laws and Regulations

China has advanced some of the first AI laws and regulations at the national level, summarised in Table 2. Unlike the horizontal risk-based approach of the EU, China has favoured the sector-specific US approach of laws tailored to specific use cases. Despite appearances of centralised government control, Chinese AI regulations are the product of an iterative process involving diverse stakeholders including mid-level bureaucrats, academics, corporations, startups, and think tanks.[42] The central government relies upon a pipeline of experts to formulate and interpret the details, while local officials mainly ensure alignment with Chinese and socialist ideology.[43]

Date	Title	Issuing Body	Description
June 2017	Cybersecurity Law	National People's Congress	Legal frameworks for cybersecurity, data protection, and network security, indirectly impacting AI.
Sept. 2021	Data Security Law	National People's Congress	Regulations on data processing and security affecting AI systems.
Nov. 2021	Personal Information Protection Law (PIPL)	National People's Congress	Comprehensive data privacy law governing collection, storage, and transfer of personal information.
Mar. 2022	Algorithm Recommendation Regulation	CAC	Regulates recommendation algorithms, requiring transparency and fairness.
Jan. 2023	Deep Synthesis Regulation	CAC	Governs generative AI, focusing on authenticity and traceability of AI-generated content.
Aug. 2023	Generative AI Measures	CAC and six other authorities	Obligations on generative AI service providers for legality, fairness, and cybersecurity.

Table 2: Chinese AI laws and regulations.

6.3 Registration, Compliance, and Industrial Policy

On paper, China has perhaps the most onerous AI regulation requirements of the three regions considered. Model registration, data management rules, and ongoing compliance monitoring illustrate how strict central regulation can slow innovation. As of March 2024, only 546 AI models had been registered, and just seventy were Large Language Models,[44] in stark contrast to the over 500,000 open-source LLMs on Huggingface.co,[45] which is banned in China.[46]

Yet in practice, enforcement is deliberately selective. China's 'Made In China 2025' industrial policy supports 10,000 'Little Giants', small and mid-sized enterprises recognised as key sources of innovation,[47] which are informally afforded regulatory leeway.[48] Startups and SMEs largely operate beneath the enforcement threshold as long as they lack a large public presence.[49] Selective enforcement is also accompanied by a growing network of municipal AI regulatory sandboxes. Shanghai and Shenzhen have both established AI pilot zones that allow companies to test novel AI applications under relaxed compliance requirements, mirroring the EU AI Act's sandbox provisions but with characteristically less formal structure. The Shanghai AI pilot zone, for instance, permits experimentation with autonomous driving, medical AI diagnostics, and smart-city applications under streamlined registration procedures, providing a controlled pathway for innovation that the national regulatory framework does not yet accommodate.

China's selective approach also has an international dimension. Through the Belt and Road Initiative's digital infrastructure investments, Chinese AI companies, and the regulatory norms embedded in their systems, are being exported to Southeast Asia, Central Asia, and Africa. Smart-city platforms built by Huawei and Alibaba, surveillance systems incorporating Chinese AI, and telecommunications infrastructure carrying Chinese technical standards extend China's cyber governance model far beyond its borders.[50] The result is a de facto 'Beijing Effect' in AI governance: developing nations that adopt Chinese-built AI infrastructure implicitly adopt the data governance and content-control frameworks embedded within it, often without the explicit legislative adoption that characterises the Brussels Effect.

The foundational layer of this ecosystem predates AI-specific regulation by several years. The 2017 Cybersecurity Law, the 2021 Data Security Law, and the Personal Information Protection Law (PIPL) established a comprehensive data governance architecture, covering collection, storage, cross-border transfer, and security, within which AI-specific regulations now operate.[51] The CAC's algorithm registration system, which requires companies to disclose the logic and parameters of recommendation algorithms, functions simultaneously as an AI governance mechanism and a tool for ensuring that algorithmic systems do not undermine social stability or state information-control objectives. For international firms, compliance with China's AI regulations necessarily entails compliance with its broader cybersecurity and data-localisation requirements, a coupling that neither the EU nor the US imposes with comparable institutional force.

6.4 Recent Developments (2025)

Two developments in 2025 deepened the integration of AI governance within China's cybersecurity architecture. In August, the State Council issued the 'AI Plus' Action Plan,[52] an industrial policy targeting 70% AI penetration across key economic sectors by 2027, framing AI adoption as a matter of national competitiveness. More consequentially for cyber governance, the National People's Congress amended the Cybersecurity Law in October[53] to incorporate AI governance provisions for the first time in primary national legislation. The amendments mandate AI ethics review and risk assessment for systems deployed in critical infrastructure, increase administrative penalties tenfold (from RMB 1 million to RMB 10 million), and grant the CAC expanded enforcement authority over AI systems that process personal data or affect network security. Mandatory AI content-labelling rules also took effect in September 2025. The institutional logic is clear: AI governance is not a separate policy domain but an extension of the cybersecurity and data-sovereignty framework that the CAC already administers.

7 United States

7.1 Overview

On 30 October 2023, President Biden signed Executive Order #14110 on the 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence'.[54] EO #14110 delegated AI responsibilities to over fifty existing federal agencies with over one hundred specific tasks, moving beyond the voluntary commitments secured in July 2023[55] and the October 2022 AI Bill of Rights.[56]

7.2 Laws and Regulations

The US regulatory tradition emphasises decentralised oversight: Congress passes framework legislation, and specialised federal agencies enforce rules within their domains.[57][58][59] Technology regulation has historically combined legislative action, executive orders, agency rulemaking, and industry self-regulation.[60][61] This distributed approach reflects both philosophical distrust of centralised power and the practical influence of a $46 billion lobbying industry.[62]

EO #14110 was somewhat exceptional: the executive branch initiated AI-related policies partly due to its ability to respond more quickly than Congress. In contrast to the more centralised approaches of the EU and China, the order nonetheless reflected the distinct US approach of delegating specific objectives to agencies with pre-existing domain expertise.[63]

7.3 Executive Order 14110

EO #14110 directed over fifty federal agencies to take over one hundred specific actions addressing eight core policy areas including safety and security, innovation and competition, worker support, bias and civil rights, consumer protection, privacy, federal use of AI, and international leadership.[64] Both the 180-day and 270-day deadlines were met.[65][66]

EO #14110 addressed many core concerns highlighted in the EU AI Act but with key differences.[67] Where the EU established a new centralised authority (the AI Office), the US augmented existing federal agencies. The US approach was arguably more immediately actionable but also more vulnerable to political reversal, a vulnerability dramatically demonstrated in January 2025.

Within this structure, the National Institute of Standards and Technology (NIST) established the US AI Safety Institute in January 2024,[68] with task forces focusing on safety, evaluation, measurement, and risk management.[69]

7.4 AI and Cybersecurity Governance

Unlike the EU's integrated approach through the AI Act and NIS2, the United States lacks a unified framework connecting AI governance with cybersecurity policy. Before its revocation, EO #14110 assigned cybersecurity-related AI tasks to multiple agencies: NIST was directed to develop AI red-teaming standards and adversarial testing guidelines; the Department of Homeland Security (DHS) was tasked with assessing AI-related threats to critical infrastructure; and the Cybersecurity and Infrastructure Security Agency (CISA) published its 'Roadmap for Artificial Intelligence' in late 2023, identifying AI as both an essential tool for cyber defence and a vector for novel threats. Meanwhile, the Department of Defence's Replicator initiative committed to fielding autonomous AI-enabled systems at scale, raising governance questions about autonomous cyber operations that no civilian regulatory framework addresses.

Spread across NIST, CISA, DHS, DOD, and sector-specific agencies, this distributed approach produced rapid progress under EO #14110's coordination mandate. But it also created a structural vulnerability: because coordination depended on presidential direction rather than legislative authority, the entire framework was susceptible to political reversal.

7.4.1 Revocation and Its Cyber Governance Consequences

It was realised on 20 January 2025, when President Trump revoked EO #14110 on his first day in office. His replacement order, EO 14179 ('Removing Barriers to American Leadership in Artificial Intelligence'),[70] establishes a policy of sustaining US AI dominance through economic competitiveness and national security, but contains no cybersecurity requirements, inter-agency coordination mandates, safety benchmarks, or compliance deadlines. The 180-day AI Action Plan it mandates had, as of late 2025, not addressed the cybersecurity dimensions that EO #14110 had begun to operationalise.

The consequences for US cyber governance are immediate. CISA's AI Roadmap lacks binding authority without executive-level backing. NIST's AI Safety Institute continues to operate but with a significantly narrowed mandate. The result is a governance vacuum in which AI-cybersecurity coordination depends on agency initiative rather than presidential direction, precisely as AI-enabled cyber threats are proliferating. This vacuum is a stark expression of the US position in the trilemma: by prioritising innovation speed through deregulation, the Trump administration has simultaneously weakened the coherence of federal AI-cybersecurity governance.

7.5 California SB 1047 and State-Level Regulation

California Senate Bill 1047, introduced in February 2024, attempted to establish a regulatory framework for 'frontier models' defined by computational resources.[71] The bill attracted both broad support and vigorous opposition.[72][73] Governor Newsom vetoed SB 1047 on 29 September 2024[74] because he opposed standards solely based on model size, favouring instead assessment of deployment contexts. The episode shows the gravitational pull of institutional traditions: even ambitious ex ante proposals get reshaped by the US system's preference for ex post, risk-based approaches.

The SB 1047 debate catalysed a wave of state-level AI legislation in 2025. California enacted SB 53, the Transparency in Frontier Artificial Intelligence Act,[75] on 29 September 2025. SB 53 shifts from prescriptive safety mandates to a transparency-centred approach: developers of frontier models (trained at $> 10^{26}$ operations) must publish annual risk-governance frameworks, issue pre-deployment transparency reports, and report critical safety incidents within 15 days. New York followed with the RAISE Act[76] in December 2025, requiring annual independent audits and 72-hour incident reporting. Together, these laws suggest that US AI governance is settling on transparency and disclosure obligations rather than ex ante safety requirements.

8 Discussion: The Cyber Governance Trilemma

8.1 Comparative Synthesis

Applying the governance typology introduced in Section 2, a clear pattern emerges. The EU occupies the centralised, ex ante quadrant: the AI Act establishes a unified, risk-based framework that regulates AI systems *before* they reach the market, enforced through a new centralised authority. The US occupies the distributed, ex post quadrant: even before the revocation of EO #14110, the US relied heavily on industry self-regulation and existing legal frameworks. China occupies a hybrid position: centralised guidance and registration requirements coexist with decentralised, sector-specific enforcement and deliberate regulatory forbearance for innovative SMEs.

These divergent positions produce what we term the *cyber governance trilemma*. Drawing on the international political economy literature on 'impossible trinities', we argue that jurisdictions cannot simultaneously optimise three desirable objectives:

1. **Innovation speed**: minimising regulatory barriers to AI development and deployment.

2. **Safety and rights protection**: ensuring AI systems do not cause harm, discrimination, or rights violations.

3. **Regulatory interoperability**: maintaining compatibility with other jurisdictions' frameworks to enable cross-border operations.

The trilemma is not merely an empirical coincidence—it reflects a structural incompatibility among the three objectives, operating through three bilateral tensions.

The *innovation–safety tension* is the most widely discussed: stringent ex ante regulation requires developers to demonstrate compliance before deployment, adding time and cost that directly reduce innovation speed. The EU's conformity assessment regime for high-risk AI systems illustrates this clearly: providers must complete risk assessments, establish quality management systems, and maintain technical documentation before market access, a process that delays deployment relative to jurisdictions without such requirements. Conversely, permissive regulation accelerates deployment but increases harm probability, as the US experience with largely unregulated AI-enabled content recommendation systems and deepfake generation tools demonstrates.

The *safety–interoperability tension* is less intuitive but equally consequential. Stronger domestic safety standards inevitably diverge from other jurisdictions' definitions of acceptable risk, creating regulatory walls that impede cross-border AI operations. China's content-labelling requirements for AI-generated material are structurally incompatible with EU transparency standards, which focus on system-level risk classification rather than content-level marking. The more rigorously a jurisdiction specifies safety requirements, and the more those requirements reflect domestic political values, the greater the divergence from jurisdictions with different risk tolerances.

The *innovation–interoperability tension* operates through the Brussels Effect mechanism itself. Establishing global regulatory standards requires comprehensive, prescriptive rules with extraterritorial reach; but such rules constrain domestic innovators who must comply with standards designed for international projection. The EU's GPAI provisions have drawn criticism for imposing compliance burdens on European open-source AI developers that their US and Chinese competitors do not face, potentially deterring the very innovation that global standard-setting requires.

The structural cause of the trilemma is that AI governance involves distributional choices—who bears risk, who captures economic value, who sets international norms—that map onto incompatible political economy preferences across jurisdictions. No single regulatory design can simultaneously minimise barriers to innovation, maximise safety guarantees, and maintain cross-border regulatory compatibility, because each objective demands institutional choices that work against the other two.

Each jurisdiction therefore sacrifices one objective, as summarised in Table 3. The EU prioritises safety and interoperability (through its Brussels Effect ambitions) at the cost of innovation velocity. The US, particularly after the revocation of EO #14110, prioritises innovation speed at the cost of consistent safety guarantees. China prioritises innovation speed and selective safety enforcement at the cost of international interoperability, embedding AI governance within a cyber sovereignty strategy that is structurally incompatible with multi-stakeholder governance models.[77]

The Brussels Effect thesis receives only partial support from this analysis. The EU AI Act's

Jurisdiction	Innovation	Safety/Rights	Interoperability
European Union	Constrained	Strong (ex ante)	High (Brussels Effect)
United States	Prioritised	Weak (post-EO revocation)	Moderate
China	Prioritised (selective)	Selective enforcement	Low (cyber sovereignty)

Table 3: The cyber governance trilemma: how each jurisdiction resolves the innovation–safety–interoperability trade-off.

extraterritorial reach creates compliance incentives for global firms, but the simultaneous emergence of substantive frameworks in both the US and China limits the unilateral standard-setting power that the EU enjoyed with the GDPR. AI governance is evolving towards a *multipolar regulatory landscape*[78] in which firms must navigate competing compliance regimes, a pattern that mirrors the broader fragmentation of internet governance.[79]

8.2 Implications for International Cyber Governance

Regulatory fragmentation carries several concrete implications for the international cyber governance community.

Regulatory fragmentation as systemic cyber risk. Divergent AI governance frameworks create compliance gaps: seams between regulatory regimes that well-resourced threat actors can exploit. Where AI systems in critical infrastructure must satisfy different safety standards depending on jurisdiction, the weakest link determines the overall cyber resilience of interconnected systems. The interaction between the EU's AI Act and NIS2 Directive illustrates the emerging model of integrated AI-cybersecurity governance, but no comparable integration exists at the international level.

Implications for the transatlantic relationship and China. The Trump administration's revocation of EO #14110 widened the regulatory gap between the US and EU precisely as the AI Act entered enforcement. European firms operating in the US face declining regulatory certainty, while US firms must still comply with the AI Act for EU market access. Meanwhile, China's integration of AI governance into its Cybersecurity Law creates a self-contained regulatory ecosystem that reinforces cyber sovereignty, complicating already-fraught US–China technology competition and multilateral cyber norm processes.

Model adoption by developing nations. For developing countries that lack the institutional capacity to design bespoke AI governance frameworks, the choice between regulatory models carries significant geopolitical implications.[80][81] The GDPR experience, in which over 130 countries adopted data protection laws influenced by the EU model, suggests that many countries will align with one of the three major AI regulatory frameworks. Early evidence confirms this pattern but also reveals more complex dynamics than simple emulation.

Brazil's AI regulatory framework, approved by the Senate in December 2024, draws heavily on the EU AI Act's risk-based classification system while incorporating provisions for algorithmic impact assessments tailored to the country's acute concerns about racial and socioeconomic discrimination. India's proposed Digital India Act takes a different path, emphasising light-touch regulation and industry self-governance that more closely resembles the US approach, reflecting India's ambition to position itself as a global AI development hub. Singapore's Model AI Governance Framework, now in its third iteration, represents a pragmatic middle ground: voluntary guidelines grounded in risk assessment and transparency principles, designed to attract international AI investment without imposing compliance burdens that would deter firms from establishing regional headquarters.

At the multilateral level, the African Union's Continental AI Strategy (2024) and the ASEAN Guide on AI Governance and Ethics both signal a preference for principles-based frameworks that preserve regulatory flexibility; but the practical governance choices of individual member states are increasingly shaped by which major power provides their AI infrastructure. For cyber governance, this 'regulatory template' dynamic is consequential: developing nations' choices about AI regulation determine their alignment in international cyber norm debates, including their positions in the UN Open-Ended Working Group on Information and Communications Technologies and the Global Digital Compact. The trilemma thus operates not only within the three major jurisdictions but across the entire global governance architecture, as regulatory choices cascade through investment relationships, infrastructure dependencies, and multilateral alignments.

Implications for international norm-building. The trilemma complicates ongoing efforts to establish international AI governance norms through the United Nations and other multilateral forums. If the three major AI powers cannot agree on basic regulatory approaches (ex ante versus ex post, centralised versus distributed, rights-based versus innovation-first), the prospects for a binding international AI governance regime remain limited. More realistic pathways may include issue-specific agreements (on autonomous weapons, deepfakes, or AI-enabled cyber operations), mutual recognition frameworks, or informal convergence through regulatory competition.

8.3 AI Governance and Cyber Conflict

The cyber governance trilemma extends beyond civilian AI regulation into the military and security domain, where the stakes are highest and the governance gaps most consequential. AI-enabled capabilities are transforming cyber operations across all three jurisdictions: automated vulnerability discovery, AI-generated spear-phishing at scale, autonomous network penetration tools, and machine-speed decision-making in cyber defence all blur the boundary between civilian AI governance and military cyber operations.[82]

Each jurisdiction's regulatory framework handles this boundary differently, and problematically. The EU AI Act explicitly exempts national security and defence applications from its scope, creating a regulatory gap in which military AI systems face no comparable governance framework at the European level. China's military-civil fusion strategy deliberately erases the distinction between civilian and military AI development: technologies developed under civilian AI regulations are systematically channelled into People's Liberation Army modernisation programmes, meaning that China's ostensibly civilian AI governance framework has direct military implications that neither the EU nor the US regulatory frameworks account for. The United States, through programmes such as the Department of Defence's Replicator initiative and DARPA's AI-enabled cyber operations research, is developing autonomous systems that operate in a governance grey zone between EO 14179's civilian innovation mandate and the Laws of Armed Conflict.

The trilemma applies to military AI governance with particular force. No jurisdiction can simultaneously pursue AI-enabled military advantage (innovation), compliance with international humanitarian law and arms-control norms (safety), and interoperability with allies' autonomous systems (interoperability). The UN Group of Governmental Experts on Lethal Autonomous Weapons Systems and the Open-Ended Working Group on ICT security have both struggled to establish meaningful norms precisely because the three major AI powers approach military AI governance from incompatible positions. Issue-specific agreements (on autonomous cyber weapons, AI-generated disinformation in armed conflict, or machine-speed escalation dynamics) may represent the most achievable near-term pathway, but even these require a degree of regulatory convergence that the trilemma structurally impedes.

9 Conclusion

The EU, China, and the United States are constructing fundamentally different AI regulatory systems, each reflecting distinct institutional traditions, political values, and geopolitical ambitions. The resulting regulatory fragmentation is not merely an inconvenience for global firms—it is a structural feature of cyber governance that shapes cybersecurity, international cooperation, and the distribution of technological power. As AI capabilities advance and become more deeply embedded in critical systems, the trilemma will only sharpen. How different jurisdictions resolve the tensions between innovation, safety, and interoperability will determine the shape of international cyber governance for decades to come.

Author Contributions

Jon Chun led the comparative analysis of the United States and China, the cyber governance trilemma framework, and the regulatory timeline dataset. Christian Schroeder de Witt led the analysis of the European Union and the regime complexity framing. Katherine Elkins contributed to the United States analysis and the developing-nations implications. All authors contributed to the theoretical framework, methodology, and comparative synthesis.

About the Authors

Jon Chun is Visiting Instructor of Humanities at Kenyon College, with graduate degrees in computer science and electrical engineering from UC Berkeley and UT Austin and extensive industry experience in FinTech and cybersecurity. He is lead investigator for the Modern Language Association's participation in the NIST US AI Safety Institute and co-principal investigator on an IBM–Notre Dame Tech Ethics Lab grant examining AI decision-making in criminal justice contexts. His research encompasses human-centred AI, AI safety, and technology policy.

Christian Schroeder de Witt is Lecturer in the Department of Engineering Science at the University of Oxford and Principal Investigator of the Oxford Witt Lab for Trust in AI (OWL). A Royal Academy of Engineering Research Fellow and Schmidt Sciences AI2050 Fellow, his research addresses multi-agent security and AI assurance, examining how decentralised AI systems can be secured against emerging threats. He serves as an expert adviser to RAND, the BBC, and the UK government on AI governance and risk.

Katherine Elkins is Professor of Comparative Literature and Humanities at Kenyon College, with affiliated faculty status in Computing. She co-founded Kenyon's human-centred AI curriculum in 2016 and serves as co-principal investigator for both the NIST US AI Safety Institute and the IBM–Notre Dame Tech Ethics Lab grant on AI decision-making in recidivism cases. Her research bridges computational methods with humanistic inquiry to inform policy on AI safety, bias, and governance.

Notes

[1] Lucas Kello. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.

[2] Joseph S. Nye Jr. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series No. 1. 2014. URL: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/.

[3] Dennis Broeders. "Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security". In: *Journal of Cyber Policy* 2.3 (2017), pp. 272–296. DOI: 10.1080/23738871.2017.1403640.

[4] Corinne Cath et al. "Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach". In: *Science and Engineering Ethics* 24.2 (2018), pp. 505–528. DOI: 10.1007/s11948-017-9901-7.

[5] Luciano Floridi et al. "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations". In: *Minds and Machines* 28.4 (2018), pp. 689–707. DOI: 10.1007/s11023-018-9482-5.

[6] Charlotte Stix. "Actionable Principles for Artificial Intelligence Policy: Three Pathways". In: *Science and Engineering Ethics* 27.1 (2021), p. 15. DOI: 10.1007/s11948-020-00277-3.

[7] Nathalie A. Smuha. "From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence". In: *Law, Innovation and Technology* 13.1 (2021), pp. 57–84. DOI: 10.1080/17579961.2021.1898300.

[8] Michael Veale and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach". In: *Computer Law & Security Review* 22 (2021), p. 105573. DOI: 10.1016/j.clsr.2021.105573.

[9] Huw Roberts et al. "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation". In: *AI & Society* 36.1 (2021), pp. 59–77. DOI: 10.1007/s00146-020-00992-2.

[10] Inga Ulnicane et al. "Framing Governance for a Contested Emerging Technology: Insights from AI Policy". In: *Policy and Society* 40.2 (2021), pp. 158–177. DOI: 10.1080/14494035.2020.1855800.

[11] Cath et al., see n. 4.

[12] Ulnicane et al., see n. 10.

[13] Smuha, see n. 7.

[14] Anu Bradford. "The Brussels Effect: How the European Union Rules the World". In: *Faculty Books* (Mar. 2020). DOI: https://doi.org/10.1093/oso/9780190088583.001.0001. URL: https://scholarship.law.columbia.edu/books/232.

[15] Giandomenico Majone. "The Rise of the Regulatory State in Europe". In: *West European Politics* 17.3 (1994), pp. 77–101. DOI: 10.1080/01402389408425031.

[16] David Levi-Faur. "The Global Diffusion of Regulatory Capitalism". In: *The Annals of the American Academy of Political and Social Science* 598.1 (2005), pp. 12–32. DOI: 10.1177/0002716204272371.

[17] Stix, see n. 6.

[18] Veale and Borgesius, see n. 8.

[19] Roberts et al., see n. 9.

[20] Nye, see n. 2.

[21] Milton L. Mueller. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity Press, 2017.

[22] Laura DeNardis. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.

[23] Kristen E. Eichensehr. "The Cyber-Law of Nations". In: *Georgetown Law Journal* 108.2 (2019), pp. 317–380.

[24] Smuha, see n. 7.

[25] European Union. *Regulation (EU) 2024/123 of the European Parliament and of the Council of 21 May 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Accessed: 2024-09-08. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[26] European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Article 7*. Accessed: 2024-09-08. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[27] Leila Abboud and Javier Espinoza. "EU's new AI Act risks hampering innovation, warns Emmanuel Macron". In: *Financial Times* (Dec. 2023). URL: https://www.ft.com/content/9339d104-7b0c-42b8-9316-

72226dd4e4c0 (visited on 09/08/2024).

[28] Billy Perrigo. *Exclusive: OpenAI Lobbied E.U. to Water Down AI Regulation*. en. June 2023. URL: https://time.com/6288245/openai-eu-lobbying-ai-act/ (visited on 09/08/2024).

[29] LAION. *A Call to Protect Open-Source AI in Europe | LAION*. en. 2023. URL: https://laion.ai/notes/letter-to-the-eu-parliament (visited on 09/08/2024).

[30] The Privacy Advisor Podcast. *The Privacy Advisor Podcast: Inside the EU AI Act negotiations: A discussion with Laura Caroli*. en. 2024. URL: https://privacyadvisorpodcast.libsyn.com/inside-the-eu-ai-act-negotiations-a-discussion-with-laura-caroli (visited on 09/08/2024).

[31] European Parliament and Council of the European Union. *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act)*. Official Journal of the European Union, L 265/1, 12 October 2022. 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925.

[32] European Parliament and Council. *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)*. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[33] Chatham House. *The EU's new AI Act could have global impact | Chatham House – International Affairs Think Tank*. en. Mar. 2024. URL: https://www.chathamhouse.org/2024/03/eus-new-ai-act-could-have-global-impact (visited on 09/08/2024).

[34] Bradford, see n. 14.

[35] Marco Almada and Anca Radu. "The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy". en. In: *German Law Journal* (Feb. 2024), pp. 1–18. ISSN: 2071-8322. DOI: 10.1017/glj.2023.108. URL: https://www.cambridge.org/core/journals/german-law-journal/article/brussels-sideeffect-how-the-ai-act-can-reduce-the-global-reach-of-eu-policy/032C72AEC537EBB6AE96C0FD90387E3E (visited on 09/08/2024).

[36] European Commission. *European AI Office | Shaping Europe's digital future*. en. 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/ai-office (visited on 09/08/2024).

[37] European Union, *Regulation (EU) 2024/123 of the European Parliament and of the Council of 21 May 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, see n. 25, Article 5.

[38] European Union, *Regulation (EU) 2024/123 of the European Parliament and of the Council of 21 May 2024*

Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), see n. 25, Article 6.

[39] European Union, *Regulation (EU) 2024/123 of the European Parliament and of the Council of 21 May 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, see n. 25.

[40] European Union, *Regulation (EU) 2024/123 of the European Parliament and of the Council of 21 May 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, see n. 25, Article 53–54.

[41] A. Zhang. *High Wire: How China Regulates Big Tech and Governs Its Economy*. Oxford University Press, 2022.

[42] Matt Sheehan. "Tracing the Roots of China's AI Regulations". In: *Carnegie Endowment for International Peace* (Feb. 2024). Accessed: May 2, 2024. URL: https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815.

[43] Zhang, see n. 41.

[44] China Money Network. "Chinese tech giants dominate AI algorithms with a focus on industry-specific applications". In: *China Money Network* (Mar. 2024). Accessed: May 2, 2024. URL: https://www.chinamoneynetwork.com/2024/03/07/chinese-tech-giants-dominate-ai-algorithms-with-a-focus-on-industry-specific-applications.

[45] Huggingface.co. *Models*. Accessed: May 2, 2024. May 2024. URL: https://huggingface.co/models.

[46] ChinaTalk. "Hugging Face Blocked! 'Self-Castrating' China's ML Development + Jordan at APEC". in: *ChinaTalk* (Oct. 2023). Accessed: May 2, 2024. URL: https://www.chinatalk.media/p/hugging-face-blocked-self-castrating.

[47] Global Times. "China to develop 10,000 'little giants' in push for advanced manufacturing". In: *GlobalTimes.cn* (July 2021). Accessed: May 2, 2024. URL: https://www.globaltimes.cn/page/202107/1227877.shtml.

[48] Angela Huyue Zhang. *How China Regulates Big Tech and Governs AI*. Philip K.H. Wong Centre for Chinese Law [Video]. YouTube. Accessed: May 2, 2024. Mar. 2024. URL: https://www.youtube.com/watch?v=NS1DGd2IXDs.

[49] Zhang, see n. 41.

[50] Roberts et al., see n. 9.

[51] Roberts et al., see n. 9.

[52] State Council of the People's Republic of China. *AI Plus Action Plan*. Issued August 27, 2025. 2025. URL: https://english.www.gov.cn/policies/latestreleases/202508/27/content_WS68ae7976c6d0868f4e8f51a0.html.

[53] National People's Congress Standing Committee. *Amendments to the Cybersecurity Law of the People's Republic of China*. Passed October 28, 2025; effective January 1, 2026. 2025.

[54] The White House. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Accessed: 2024-09-25. Oct. 2023. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[55] The White House. *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*. Accessed: 2024-05-02. July 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

[56] The White House. *Blueprint for an AI Bill of Rights*. Accessed: 2024-05-02. Oct. 2022. URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[57] National Science Foundation. *About*. Accessed: July 16, 2024. 2024. URL: https://new.nsf.gov/about.

[58] Security and Exchange Commission. *About and Mission*. Accessed: July 16, 2024. 2024. URL: https://www.sec.gov/about/mission.

[59] Environmental Protection Agency. *About Page, Our Mission and What We Do*. Accessed: July 16, 2024. 2024. URL: https://www.epa.gov/aboutepa/our-mission-and-what-we-do.

[60] M. A. Cusumano, A. Gawer, and D. B. Yoffie. "Social Media Companies Should Self-Regulate. Now". In: *Harvard Business Review* (Jan. 2021). URL: https://hbr.org/2021/01/social-media-companies-should-self-regulate-now.

[61] M. Minow and N. Minow. "Social Media Companies Should Pursue Serious Self-Supervision— Soon: Response to Professors Douek and Kadri". In: *Harvard Law Review* (June 2023). URL: https://harvardlawreview.

org/forum/vol-136/social-media-companies-should-pursue-serious-self-supervision-soon-response-to-professors-douek-and-kadri/.

[62] Anna Massoglia. "State and federal lobbying spending tops $46 billion after federal lobbying spending broke records in 2023". In: *OpenSecrets.com* (Jan. 2024). URL: https://www.opensecrets.org/news/2024/01/state-and-federal-lobbying-spending-tops-46-billion-after-federal-lobbying-spending-broke-records-in-2023.

[63] Perkins and Coie. *States Begin to Regulate AI in the Absence of Regulation*. Accessed: July 16, 2024. May 2024. URL: https://www.perkinscoie.com/en/news-insights/states-begin-to-regulate-ai-in-absence-of-federal-legislation.html.

[64] The White House. *Administration Actions on AI*. Accessed: 2024-09-25. Mar. 2024. URL: https://ai.gov/actions/.

[65] The White House. *Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order*. Accessed: 2024-05-02. Apr. 2024. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/29/biden-harris-administration-announces-key-ai-actions-180-days-following-president-bidens-landmark-executive-order/.

[66] The White House. *Fact Sheet: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitment on AI*. Accessed: 2024-09-25. July 2024. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announces-new-ai-actions-and-receives-additional-major-voluntary-commitment-on-ai/.

[67] Congressional Research Service. *Highlights of the 2023 Executive Order on Artificial Intelligence for Congress*. Accessed: May 2, 2024. 2024. URL: https://crsreports.congress.gov/product/pdf/R/R47843/8.

[68] NIST. *About*. Accessed: July 16, 2024. 2024. URL: https://www.nist.gov/about-nist.

[69] NIST. *AI Risk Management Framework*. Accessed: July 16, 2024. 2024. URL: https://www.nist.gov/itl/ai-risk-management-framework.

[70] The White House. *Removing Barriers to American Leadership in Artificial Intelligence*. Executive Order 14179, January 23, 2025. 2025. URL: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

[71] LegiScan. *California Senate Bill 1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*. Accessed: May 1, 2024. 2024. URL: https://legiscan.com/CA/text/SB1047/2023.

[72] The Hill. "AI Employees Support California AI Bill". In: *The Hill* (2024). Accessed: 2024-01-15. URL: https://thehill.com/policy/technology/4869225-ai-employees-support-california-ai-bill/.

[73] Mi. Nunez. *AI safety showdown: Yann LeCun slams California's SB 1047 as Geoffrey Hinton backs new regulations*. Accessed: 2024-09-18. Sept. 2024. URL: https://venturebeat.com/ai/ai-safety-showdown-yann-lecun-slams-californias-sb-1047-as-geoffrey-hinton-backs-new-regulations/.

[74] Gavin Newsom. *Office of the Governor*. Accessed: 2024-09-23. 2024. URL: https://www.gov.ca.gov/wp-content/uploads/2024/09/SB-1047-Veto-Message.pdf.

[75] State of California. *SB 53: Transparency in Frontier Artificial Intelligence Act*. Signed September 29, 2025. 2025. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53.

[76] State of New York. *The RAISE Act (AB 6453/SB 6953)*. Signed December 19, 2025. 2025. URL: https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-require-ai-frameworks-ai-frontier-models.

[77] Mueller, see n. 21.

[78] Smuha, see n. 7.

[79] Nye, see n. 2.

[80] DeNardis, see n. 22.

[81] Madeline Carr. "Public–Private Partnerships in National Cyber-Security Strategies". In: *International Affairs* 92.1 (2016), pp. 43–62. DOI: 10.1111/1468-2346.12504.

[82] Kello, see n. 1.