Near to Midterm Risks and Opportunities of Open Source Generative AI

TODO:

* Update old text (see notes herein)
* Reformat old text to fit into this format
* Add REFERENCES
* Post ot ArXiv
* 1+ Follow-up paper(s)

==================================================

Updates and Corrections to Existing Sections

==================================================

Paper Notes:

Color Codes:

Blue : add citation

Red: edit, delete, or add text

+

### **ABSTRACT**

There are complex risk-reward trade-offs in the rapid progress and deployment of AI. As a powerful dual-use technology, it offers both immense benefits and worrisome societal risks. In response, numerous governing bodies around the world are developing a diverse range of regulatory AI laws and policies. This paper compares the three distinct approaches taken by the EU, US, and China. Together they represent leading initiatives in both AI development and AI regulation. Nonetheless each of these three emerging regulatory systems reflect distinct cultural, political and economic perspectives. The differing AI regulation frameworks also highlight differing regional perspectives with regard to the regulatory risk-benefit tradeoffs. These differing frameworks reflect different stances on the balance between upon safety versus innovation, cooperation versus competition, and trust in centralized authority versus decentralized self-interested stakeholders. The EU and US also serve as influential reference points for many other countries, like Brazil and Japan, that are forming their own AI regulatory policies. At the same time, rising US-China tension may shift the regulatory AI risk-reward calculation in the near future.

### **UPDATES/EDITS to original doc**

P3/C2/L161:

Growing economic threat

P4/C1/167:

INSERT new paragraph:

Concern over China’s growing economic in strategic technologies outlined in their China 2015 report and commercial dominance worldwide via the Belt and Road Initiative.

P4/C1/L167:

Factual error: 24 Feb 2022 Russia invades Ukraine (18 mos later) 31 Aug 2023 US restricts NVIDIA/AMD chips to some Middle East countries

P4/C1/L184-187:

Closed-closed:

INSERT (after) a paragraph describing the criteria, members and controversy around those invited as Frontier Model providers

P4/C1/L217:

Explain/contrast US model prioritizing market mechanisms, self-regulation, etc

INSERT: Concerns with regulatory capture, lobbyist, ROI

Incident of OpenAI Altman lobbying for strict US regulation at same time open EU regulation as logical profit maximizing strategy corp-govt

P4/C2/L165-183:

EXPAND INTO SECTION “Multi-Level US AI Regulation”

INSERT Fig.Unified AI Regulation Timeline

* [[2402.05048] How VADER is your AI? Towards a definition of artificial intelligence systems appropriate for regulation (arxiv.org)](https://arxiv.org/abs/2402.05048)

P4/C2/L204:

UPDATE to add final approval and enforcement start date

P5/C1/L244:

INSERT BEFORE: Fig: Canonical EU AI Act Use-Case Risk Pyramid

P5/C1/L249:

Refer to Fig Use-Case Risk Pyramid

P5/C2/L245:

Clarify this statement

P5/C2/L248:

INSERT Table that enumerates all the exemptions with clarifying notes (Key info)

P5/C2/L251:

Update from LEAKED to actual to verbage/interpretation from final version

P5/C2/L265:

Update from LEAKED to actual verbiage/interpretation from final version

P6/C1/L278:

INSERT figure illustrating value chain, responsible parties, and regulatory pre-release/reporting/monitoring requirements

P6/C1/L282:

Does the final version somewhat resolve this ‘confusion’

P6/C1/L301:

Unclear to what extent this applies to open-source AI given they, like PCs, are general purpose computing/cognitive devices

P6/C1/L311:

Has the EU determined that GenAI trained on copyrighted works violate IP law? Undetermined in the US

P6/C1/L327:

UPDATE from LEAKED to final passed version with current interpretation

P6/C2/L281:

UPDATE this entire section to comport with final version

P6/C2/L300:

Confirm the final version agrees with facts/opinions in this section

P6/C2/L322:

Transatlantic agreement only apply to US-EU, not EU-rest of the world

What happens if EU becomes like China where citizen evade EU restrictions by using real-time VPNs or simply batch process data with AI offshore and only import the results diluted by some Human in the Loop mitigation workflow? Overseas subsidiaries, etc.

P6/C2/L328:

UPDATE with final version, fact check, and verify opinions on France, Germany and UK stances on final version

P7/C1/L343:

UPDATE with the final version and latest on harmonized standards

P7/C1/L350:

### **1. Governance and Geopolitics**

#### **2.2.1. Overview**

(2.1.The US Regulatory Landscape)

### **2. Regulatory Landscape**

#### **2.2.1. Overview**

#### **2.1 United States**

(2.1.The US Regulatory Landscape)

##### **2.1.1. Overview**

On October 30, 2023 US President Biden signed an executive order (EO) on the Safe,Secure,and Trustworthy Development and Use of Artificial Intelligence [cite]. The order is generally considered to represent a wide range of interests. There has been some criticism, however, about the influence of a handful of tech billionaires, with Politico detailing the extent to which certain parties were confirmed to be present at closed meetings[cite].This criticism follows on previous concern that the Congressional hearings were unduly influenced by industry given both the nature of certainremarksaswellasclosedevents--likeaprivatedinner--that was not open to review or feedback.

Ontheonehand, theUSRegulatorylandscapeevincesa holisticviewthataccountsforavarietyofinterestedparties andtriestoachieveabalancebetweenregulationandinno vationthroughresponsibleinnovation.Ontheotherhand, theUSregulatorylandscapecannotbeseenasdivorced fromthelargerlobbyingforcesunderwhichsomegroups, including theleadingindustryplayers,mayholdoutsized influence.AsHarvardscholarsSchneiderandSanderswrite, theBidenactrepresents“acontestaboutcontrolandpower, abouthowresourcesshouldbedistributedandwho should be held accountable”(?). BrendanBordelonofPolitico goesontosuggestthattheact“papersover”the“growing tensionbetweenWashington’srivalAIfactions”(?).

SchneiderandSanderscategorizethedifferentfactionsrep resentedintheexecutiveactas“doomsayers,”“reformers” and“warriors.”Doomsayershighlighttheexistentialrisk AIposes.Reformersfocusonthealreadyextantseriesof harmsbeingperpetrated,aswellaspotentialloomingeco nomicdisruption.Warriorsareconcernedwiththegeopolit icalsphereamidworriestheUSwillloseitsglobaldomi nance.Eachofthesegroupshighlightstherisksandbenefits accordingtotheirparticularconcernsandviewpoints.The doomsayershavecomeunderthemostcriticismforover statingtheextent towhichfearsofexistential riskarea dominantviewpoint amongAI researchersanddevelop ers[cite].Addingtothisconcernisthefactthathighlighting existential risk maybenefit leading industry players, for whom regulation could help as aninsincerestratagemto cement their market advantagebyhandicappingsmaller competitors.

Reflecting These Various Positions, theEOpresidentialact outlinesthevariousrisksofAIandcallsforvariousgov ernmentagenciestodevelopplansthatincludedeveloping criticalinfrastructurefordefenseandgovernmentalsupport ofAIresearch.NISTistaskedwithdevelopingpractices surroundingtheirAIRiskManagementFramework.Tothis end,NISTisintheprocessofcreatingtheUSAISafety InstituteConsortiumtoincludemembersfromstateand localgovernments,universities,non-profits,andindustry.

The Bidenand Harris Executive Order stands apart from the EU regulatory landscape in one key aspect: models with“freely available weights.”In the EU,Modelsbelow a specific compute budget threshold have been protected from regulation, at least for the present. This is seen as either a positive protection of competition and welcome development or an unfortunate capitulation to lobbying depending on the perspective. The Biden act, on the other hand,specifically calls out open-source models as a locus of potential risk.

##### **2.1.2 Laws and Regulations**

In contrast to the more centralized, top-down approach to AI regulation prioritizing safety (Europe) and social stability (China), the United States has traditionally taken a more distributed, multi-stakeholder approach to regulation. While clear directives on AI are provided by the single source of authority in the centralized political bodies of the EU and CCP, a wide range of guidelines, initiatives, laws, and other policies including trade related to AI are distributed between various federal branches, agencies and even states. This reflects the design of the American government as a balance between competing interests as well as the relatively greater mistrust of centralized authority [cite].

In the US, the legislative branch typically passes laws that form the framework for regulation, which are then enforced by the executive branch, primarily under the oversight of various federal agencies. For example, the US Congress passes laws that define specific industries or activities along with broad goals such as advancing scientific research (National Science Foundation), promoting fair markets (Securities and Exchange Commission), and safeguarding the environment (Environmental Protection Agency). Often, multiple agencies will be tasked with regulating different aspects of the same broad goal as in the Federal Trade Commission (FTC). Consumer Product Safety Commission (CPSC) and Consumer the Financial Protection Bureau (CFPB) are other agencies that specialize in different aspects of consumer protection and safety.

The rapid pace of AI innovation, the lack of technical expertise in current members of congress, and the immense potential impact of AI has reversed this normal sequence for enacting regulation moving from the legislative to executive branch. Instead, the executive branch is initiating many AI-related policies--from research to regulation--through presidential actions and executive orders. Although somewhat unique to the US, Presidential executive orders more closely match the top-down, centralized organization of the EU in Brussels and the CCP in Beijing. However, the US is still a distributed regulatory system where specific objectives are being delegated to various federal agencies, while the legislative branch tries to catch up.

##### **2.1.3 Whitehouse Executive Order 14110**

Since 2016 and over three different Presidential administrations, a number of executive orders related to AI have been issued. The Biden Whitehouse’s October 2023 “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” is the most comprehensive to date [cite1]. It directs over fifty federal agencies to take over 100 specific actions addressing eight core concerns: 1) safety and security, 2) innovation and competition, 3) worker support, 4) bias and civil rights, 5) consumer protection, 6) privacy and 7) federal use of AI [cite2].

[cite1] 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/

[cite2]

<https://ai.gov/actions/> (Biden)

This EO #14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence addresses many of the core concerns highlighted in the EU AI Act but with several key differences [cite3]. First, the EU AI Act leans towards creating new regulatory agencies, while current US strategy relies upon augmenting the extensive network of existing US federal agencies with pre-existing specialized domain expertise. Secondly, because the US approach involves over fifty federal agencies, it is much more extensive in its purview than the EU. It directly addresses broader issues like unemployment, education, research, and consumer protection. Third, again in contrast to the EU AI Act, this US strategy is arguably more immediately actionable given the over one hundred specific objectives with set deadlines delegated to federal agencies. These agencies are already specialized in a broad spectrum of existing federal government responsibilities that are being disrupted by AI. The US approach can be seen to emphasize extending expansive regulatory and legal frameworks from the ground up where infrastructure already exists, rather than creating new or overlaying regulatory frameworks in a centralized, top down fashion.

[cite3] <https://crsreports.congress.gov/product/pdf/R/R47843/8>

| **Policy Area** | **Requirements/Entities** | **Federal Entities** |
| --- | --- | --- |
| Safety and security | 27 requirements  30 entities | NIST, DOE, DOC, SRMA, Treasury, DHS, DOD, etc. |
| Innovation and competition | 21 requirements  10 entities | DOS, DHS, DOL, NSF, USPTO, HHS, VA, DOE, PCAST, OSTP+ |
| Worker support | 4 requirements  2 entities | CEA, DOL |
| Consideration of AI bias and civil rights | 9 requirements  8 entities | DOJ, OPM, HHS, USDA, DOL, HUD, DHS, OSTP |
| Consumer protection | 9 requirements  5 entities | HHS, DOT, ED, DOD, VA |
| Privacy | 6 requirements  9 entities | OMB, NIST, NSF, FPC, ICSP, DOJ, CEA, OSTP, DOE |
| Federal use of AI | 29 requirements  40 entities | OMB, OPM, CFO, GSA, etc. |
| International leadership | 6 requirements  7 entities | DOC, DOS, USAID, DHS, NIST, DOE, NSF |

**Fig.ZZ** Executive Order #14110 on the Safe, Secure, and Trustworth Development and Use of AI

Enforcement is the other major difference between the EU and the US. The EU AI Acts’ risk model is premised upon *prevention* with general guidelines, specific penalties, and centralized regulation that prohibit activities unless explicitly permitted. In contrast, the US risk model is *permissive*: it promotes innovation through competition, encourages decentralized self-regulation, and relies upon an extensive network of existing laws and regulations against abusive, illegal, and negligent practices. These networks of existing laws range over a spectrum from specific consumer production laws to general contract and tort enforcement to evolving intellectual property laws. This permissive approach follows the American tradition of tech sector self-regulation with notable success in sectors like online advertising (DAA, NAI), cybersecurity (NIST, CISA), biotechnology (IGSC, IASB), nanotechnology (ISO, NanoRisk), and cloud computing (CSA).

##### **2.1.4 Independent Federal Regulatory Bodies and Executive Branch Agencies**

The U.S. government is adopting a coordinated, whole-of-government approach to AI regulation, seeking to balance the need for innovation with the effective management of risks associated with AI technologies. A range of federal agencies, including both independent regulatory agencies and executive branch agencies, are playing critical roles in overseeing AI development, monitoring its implementation, and enforcing new AI-specific regulations. These agencies are leveraging their existing authorities to manage AI risks while also identifying areas where new regulations may be necessary.

Several **independent regulatory agencies** have been tasked with considering how to apply their oversight powers to AI. The Federal Trade Commission (FTC) is encouraged to use its existing authorities to protect consumers from potential harms arising from AI including fraud, discrimination, privacy violations, and threats to financial stability [1]. The Consumer Financial Protection Bureau (CFPB) and Federal Housing Finance Agency (FHFA) are considering ways to govern the use of AI in housing and financial markets, particularly in underwriting, valuation, and appraisal processes [1]. The Federal Communications Commission (FCC) is examining AI's impact on communications networks and consumers, including its potential for spectrum management and the prevention of unwanted robocalls and robotexts [1].

**Executive branch agencies** also have significant responsibilities in shaping AI regulation. The National Institute of Standards and Technology (NIST) is developing an AI Risk Management Framework and secure software development guidance for AI systems [1]. The Department of Commerce (DOC) is establishing reporting requirements for companies that are developing dual-use AI models. They are also engaging with international partners on AI standards development [1]. The Department of Homeland Security (DHS) is evaluating AI risks to critical infrastructure and convening an AI Safety and Security Board [1].

The overall U.S. regulatory strategy for AI involves enforcing existing technology-neutral authorities to minimize consumer harms, identify areas where new AI-specific regulations are needed, and encourage the adoption of AI risk management best practices [1]. Several key milestones and deadlines have been set, including the DOC defining conditions for AI model reporting within 90 days, incorporating NIST's AI Risk Management Framework into critical infrastructure guidelines within 180 days, mandating the adoption of these guidelines within 240 days, and publishing a global AI standards engagement plan within 270 days [1].

[1] Highlights of the 2023 Executive Order on Artificial Intelligence for Congress, Congressional Research Service, R47843, April 3, 2024.

NIST

RMF 1.0

AI Safety Institute

<https://paulfchristiano.com/>

[2018-25221.pdf (govinfo.gov)](https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf)

#### **2.2 The European Union**

(2.1.The US Regulatory Landscape)

##### **2.1.1. Overview**

(2.1.The US Regulatory Landscape)

#### **2.3 China**

##### **2.3.1. Overview**

China’s approach to AI governance and regulation is a hybrid between the centralized, top-down approach of the EU and the decentralized, free-market, competing interests model in the US. Like the EU, China emphasizes safety, individual protections, and social harmony through top-down guidance, regulation, and enforcement. Like the US, China also emphasizes bottom-up innovation and economic development with a mix of decentralized provincial control and very competitive local markets. While the EU AI Act benefits from a coherent, universal risk-based approach, the sector-specific approach locally interpreted and managed by domain regulatory experts avoids translating ambiguous language into more immediate and effective enforcement.

##### **2.3.2 Laws and Regulations**

China has advanced some of the first AI laws and regulations at the national level, which are summarized in Table X. Unlike the universal risk-based approach of the EU, China has favored the sector-specific US approach of laws tailored to specific use-cases. These specific use-cases range from those that touch on personal privacy (November 2021) to recommendation algorithms (March 2022) to generative AI (January & August 2023). Despite appearances, these regulations are the product of an iterative process involving diverse stakeholders that includes mid-level bureaucrats, academics, corporations, startups, and think tanks [Carnegie]. The central government relies upon a pipeline of these experts to formulate, clarify, and interpret the details, while they mainly concern themselves with ensuring goals and outcomes are aligned with Chinese and socialist ideology.

[Carnegie]

<https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815>

| **Date** | **Title** | **Issuing Body** | **Description** |
| --- | --- | --- | --- |
| June 1, 2017 | Cybersecurity Law | National People's Congress | Establishes legal frameworks for cybersecurity, including data protection and network security, which indirectly impact AI development and deployment. |
| September 1, 2021 | Data Security Law | National People's Congress | Provides regulations on data processing and security, affecting AI systems that process large amounts of data. |
| November 1, 2021 | Personal Information Protection Law (PIPL) | National People's Congress | China's comprehensive data privacy law that governs the collection, storage, use, and transfer of personal information, impacting AI systems that handle personal data. |
| March 1, 2022 | Algorithm Recommendation Regulation | Cyberspace Administration of China (CAC) | Regulates algorithms used for content recommendations, requiring transparency and fairness, and prohibiting practices that disrupt public order. |
| January 10, 2023 | Provisions on Management of Deep Synthesis in Internet Information Service (Deep Synthesis Regulation) | CAC | Governs generative AI technologies, focusing on the authenticity and traceability of AI-generated content to prevent misinformation. |
| August 15, 2023 | Interim Measures for the Management of Generative Artificial Intelligence Services (Generative AI Measures) | CAC and six other authorities | Targets generative AI services, imposing obligations on service providers to ensure legality, fairness, and cybersecurity of AI-generated content. |
| October 1, 2022 (Shanghai) November 1, 2022 (Shenzhen) | AI Industry Promotion Regulations in Shanghai and Shenzhen | Shanghai and Shenzhen Municipal Governments | Local regulations to promote AI development, including ethical oversight and support for innovation within the AI industry. |
| Expected in 2023 | Draft Artificial Intelligence Law (AI Law) | State Council (drafting stage) | A comprehensive national AI law is being drafted, aiming to provide an overarching legal framework for AI governance in China. |

**Table X** Chinese AI Laws and Regulations

##### **2.3.3 Registration and Compliance**

On paper China has perhaps the most onerous AI regulation requirements. TableY lists the three major steps for deploying models like Baidu’s ERNIE LLM to be in compliance with regulatory laws. These include model registration, rules for data management, and provisions for ongoing monitoring for compliance. The registration process alone illustrates how strict central regulation can slow down innovation and economic growth. As of March 2024, only 546 AI models have been registered, and just seventy are Large Language Models. This is in contrast to the countless commercial models, variants, and over 500,000 open-source LLMs on Huggingface.co (which is banned in China).

<https://www.chinamoneynetwork.com/2024/03/07/chinese-tech-giants-dominate-ai-algorithms-with-a-focus-on-industry-specific-applications#:~:text=The%20two%20latest%20batches%20in,June%20and%20August%202023%2C%20respectively>.

| **Model Registration** | |
| --- | --- |
| Approval Process | AI Models, especially Generative and LLM, must undergo through review for compliance with regulatory standards by the CAC and other bodies |
| Public Use/Licensing | After approval, all models must be registered for public use |
| Sector-Specific Approvals | Approval by additional sector-specific regulatory bodies may be required (e.g. healthcare, finance, security) |
| **Data Management** | |
| Source and Legitimacy | All training data must come from legitimate and lawful sources and be accurately labeled and documented to ensure traceability and accountability |
| Privacy Protection | All companies must comply with China’s privacy laws (e.g. PIPL) and implement robust measures to protect personal data and prevent misuse |
| Content Verification and Censorship | Providers must ensure training data does not contain prohibited data like politically sensitive or controversial content that could disrupt public order or national security (often requires moderation tools and manual checks) |
| Foreign-Language Content | Training data must include foreign language content to enhance global competitiveness |
| **Compliance Obligations** | |
| Security Assessment | Before launch, mandatory comprehensive security assessments to identify potential risks and vulnerabilities |
| Algorithm Registration | Registration of all algorithms including details on their design, functionality, and impacts on users and society |
| Ethical/Legal Compliance | Audit for compliance with ethical and legal standards, especially in avoiding inaccuracies, discrimination, and the perpetuation of biases against individual or groups |
| Ongoing Monitoring and Reporting | Continuous monitoring for system errors or deviations from approved conditions of use to allow for timely corrections |

**Table Y** AI Model Compliance Steps in China

Despite such rigorous guidelines, in practice China is relatively lax in enforcing AI regulation. This allows for the promotion of innovation, economic growth, and international competitiveness [MIT]. The “Made In China 2025” (MIC2025) plan announced in 2015 outlines strong support for innovation to help make China a global leader in AI by 2025 [cite]. Part of this plan calls for supporting 10,000 “Little Giants” - small and mid-sized enterprises (SME) recognized as a key source of innovation [cite]. Although large “National Champions” like Baidu, Tencent, and Alibaba are expected to fully comply with AI regulations because of their dominant influence, the little giants are informally afforded leeway in order to avoid heavy regulatory burdens that coul stifle innovation [cite].

[MIT]

<https://www.technologyreview.com/2024/04/09/1091004/china-tech-regulation-harsh-zhang/>

[Zhang]

<https://www.youtube.com/watch?v=NS1DGd2IXDs>

Zhang, A. (2022). Highwire: How China Regulates Big Tech and Governs Its Economy. Oxford University Press.

China’s hybrid system of AI regulation tries to capture the strengths of both the EU and the US approaches. While regulatory guidance is generally light, top-level enforcement usually comes into play when destabilizing patterns arise. This reactive enforcement can cause transitory market disruptions and lead to strict and sometimes surprisingly punitive measures to reign in excesses and outcomes at odds with CCP values like “common prosperity” [cite]. This pattern of regulatory crackdown is visible in other sectors, from real estate to education. They seem to operate to ensure more economic equality and prevent the special interest capture of government (Jack Ma’s $40B IPO of Ant Group) [cite]. To date, the hybrid strategy has been successful in guiding China to technical dominance in most of the sixty-four critical technologies tracked by the Australian Strategic Policy Institute including renewable energy, battery technology, and EVs (Gaida 2023).

##### **2.3.4 Chinese Open-Source**

The push for open-source in China can be broken down into three phases. First, acceptance into the World Trade organization in 2001 required China to take international laws on intellectual property more seriously and seek out more affordable alternatives to piracy of commercial products like Microsoft Windows OS [cite]. Second, the Edward Snowden (2013) [cite] and Wikileaks Vault 7 leaks (2017) [cite] revealed US intelligence agencies had various attacks and backdoors into leading western technologies like firmware, operating systems, smartphones, and network infrastructure. Finally, in August 2018 with the National Defense Authorization Act, Huawei and ZTE were the first in a growing list of advanced technologies under trade restrictions with China [cite].

Open-source technologies also offer China the universal benefits of greater self-reliance, cost-effectiveness, and the potential for innovation and customization. An early notable success was the open-source AndroidOS surpassing Windows in 2016 [cite]. In Q1 2024, Apple iPhone tumbled to 3rd place in the Chinese market behind domestic smartphone makers Vivo and Huawei running AndroidOS variants FuntouchOS and HarmonyOS respectively [cite]. At the time of bans on US exports of advanced Intel and AMD CPUs in December 2023, China was already shipping half of the world’s 10 billion open-source RISC-V chips by 2022 driven by $1.18B in investment [cite3].

[cite1]

https://gs.statcounter.com/os-market-share/all/china/#monthly-200901-202403

[cite2]

https://www.reuters.com/technology/apples-q1-phone-sales-china-fall-191-huaweis-up-70-2024-04-23/

[cite3]

https://www.reuters.com/technology/china-bets-open-source-chips-us-export-controls-mount-2024-02-05/

The Chinese government has supported open-source in a variety of ways. The Ministry of Industry and Information Technology published a whitepaper in July 2019 supporting open-source as central to China’s development with a recommendation to improve the ecosystem in China [cite]. In March 2021, China’s Five-Year Plan announced it would “support the development of innovative consortia such as digital technology open source communities…encourage enterprises to open up software source code, hardware designs, and application services.” [cite] At the same time, the government sponsored Gitee, an alternative to Microsoft Github for sharing, collaborating, and serving open-source software [cite]. In addition to supporting close alliances between industry and academia, the government funds open-source development through the Beijing Academy of Artificial Intelligence [cite3]. Fig.Z shows a timeline that summarizes some of the major moves towards open-source within China.

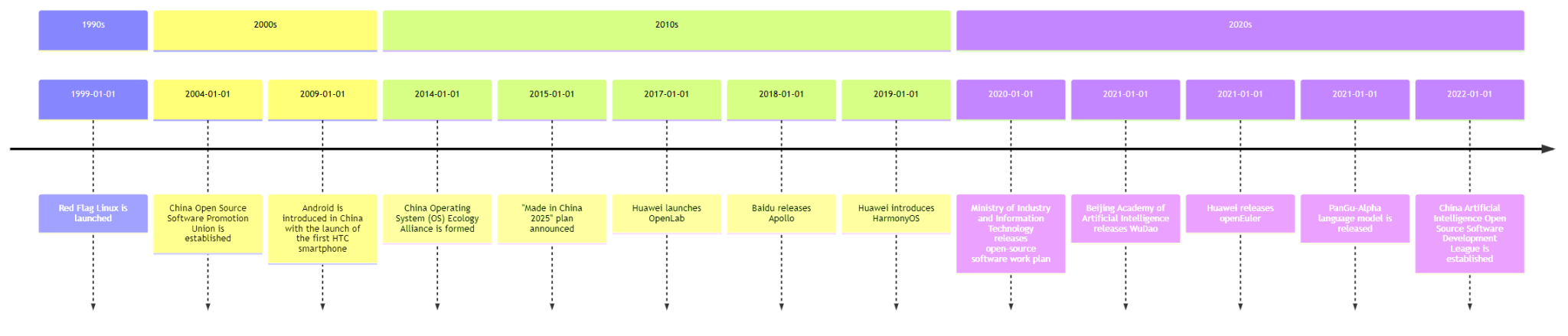
[cite]

<https://ucigcc.org/blog/chinas-uncharacteristic-approach-to-artificial-intelligence-ai-development/>

[cite]

[cite3]

https://asiasociety.org/policy-institute/chinas-emerging-approach-regulating-general-purpose-artificial-intelligence-balancing-innovation-and



**Fig.Z** Open-Source in China

##### **2.3.5 Geopolitical Tensions and the AI Regulations**

Growing trade and geopolitical tensions with the US and EU has led China to focus more urgently on developing domestic suppliers to replace key technologies that are currently under trade sanction. The US-led sanctions have denied China access to US NVIDIA high performance AI hardware, Korean Samsung and SK Hynix chips, advanced TSMC chip fabs in Taiwan, and state-of-the-art semiconductor manufacturing equipment from ASML in the Netherlands [cite]. In response, domestic Chinese chip manufacturer SMIC was able to jump from manufacturing 14nm to 7nm advanced chips within only two years and are rumored to be on the verge of mass producing 5nm chips years ahead of forecasts [cite].

Chinese AI regulations are likely to take a back seat to innovation, industrialization, and military competitiveness. This is especially true in light of a growing number of influential US politicians, who have called for overthrowing the CCP in a new Cold War 2.0 (Pottinger 2024). In recent years China has also come under increasing criticism, having been accused of potential spying (weather balloons, Tik Tok), of unfair subsidized trade/overproduction (Yellen 2024), and of military expansionism in the South China Sea and Taiwan [cite]. At the same time, AI is becoming deeply integrated into drone warfare in the Ukraine [cite], into autonomous weapons in the Gaza conflict [cite], and into F-16 fighter jet dogfights by DARPA [cite]. Both national and international cooperation on AI regulation (Bletchley 2023) are unlikely to thrive in this increasingly confrontational global environment.

### **CONCLUSION**

The EU, US, and China are each evolving distinct regulatory systems that vary in approach and emphasis. The EU AI Act proposes a coherent, universal risk-based regulatory framework with strict penalties. It is criticized, however, for stifling innovation, for ambiguous language, and for challenges in implementation details across such heterogeneous use cases. The Biden Whitehouse Executive Order on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” is the most organized plan for US AI regulation that delegates over 100 specific tasks to over 50 federal agencies to build out AI expertise and oversight according to specific domain expertise. The decentralized US approach also involves smaller regulatory initiatives by the US Congress, individual States, and even cities. This reflects the US market-driven approach of competing stakeholders. On the other hand, this approach has come under criticism for relying too heavily on self-regulation and for being open to regulatory capture. The Chinese approach to AI regulation synthesizes the US approach of use-case specific laws with a centralized and comprehensive registration, testing, and monitoring framework. At the same time, innovation and economic growth is directly and indirectly supported by initiatives like investment in thousands of ‘little dragons’ alongside relatively lax enforcement for SMEs. Critique? Growing tensions and competition between the US and China are likely to shift AI regulation towards faster innovation and away from global cooperation. In this geopolitical context, and without great incentives for global regulatory approaches, we are likely to see continued attempts to craft approaches that try to balance risk-benefit trade offs while working with the unique cultural values of each country.

**CONTRIBUTIONS**

* Christian Schroeder: The European Union
* Kathrine L. Elkins: The United States
* Jon Chun: China

Each author has approved the final version of the manuscript and agrees to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

### **REFERENCES**

The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. UK Government, [date accessed].<https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

Gaida, Dr. Jamie, Leung, Dr. Jennifer Wong, Robin, Stephan, and Cave, Danielle (2023, Sep 22) ASPI’s Critical Technology Tracker - Sensors & Biotech updates. https://www.aspi.org.au/report/critical-technology-tracker. Australian Strategic Policy Institute. (accessed 19 Apr 2024)

Pottinger, Matt and Gallagher, Mike. (2024, April 10). No substitute for victory. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/united-states/no-substitute-victory-pottinger-gallagher.

Zeng, Hui, Jingyuan Xue, Meng Hao, Chen Sun, Bin Ning and Na Zhang. “Evaluating the Generation Capabilities of Large Chinese Language Models.” *ArXiv* abs/2308.04823 (2023): n. Pag.

### **Appendix A**

US federal entities involved in the Executive Order #14110 on AI Safety:

AIM-HEAD National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity

A consortium to advance health equity and researcher diversity in AI/ML.

APDP Assistant to the President for Domestic Policy

Advises the President on domestic policy issues.

APEA Assistant to the President for Economic Affairs

Advises the President on economic policy issues.

APNSA Assistant to the President for National Security Affairs (a.k.a. the National Security Advisor)

Advises the President on national security and foreign policy issues.

CDOC Chief Data Office Council

A council that promotes data management and use within the federal government.

CEA Council of Economic Advisors

Advises the President on economic policy.

CEQ Council on Environmental Quality

Advises the President on environmental policy issues.

CISA Cybersecurity and Infrastructure Security Agency

Leads the national effort to protect and enhance the resilience of US cyber infrastructure.

DCOSP The President's Deputy Chief of Staff for Policy

Assists the President's Chief of Staff in managing the White House policy staff.

DGPC Assistant to the President and Director of the Gender Policy Council

Advises the President on gender policy issues.

DHS Department of Homeland Security

Responsible for protecting the US from threats and ensuring public safety.

DNI Director of National Intelligence (Office of the)

Oversees and directs the implementation of the National Intelligence Program.

DOC Department of Commerce

Promotes job creation, economic growth, and sustainable development in the US.

DOD Department of Defense

Responsible for national defense and military matters.

DOE Department of Energy

Ensures US energy security and promotes scientific and technological innovation.

DOJ Department of Justice

Enforces federal law and administers justice within the US.

DOL Department of Labor

Fosters and promotes the welfare of US workers, job seekers, and retirees.

DOS Department of State

Leads US foreign policy and diplomatic efforts.

DOT Department of Transportation

Oversees the nation's transportation systems and infrastructure.

ED Department of Education

Establishes policy for and administers federal aid to education.

FACA Federal Advisory Committee Act

A law that governs the operation of federal advisory committees.

FARC Federal Acquisition Regulatory Council

Assists in the direction and coordination of government-wide procurement policy.

FedRAMP Federal Risk and Authorization Management Program

A government-wide program that provides a standardized approach to cloud security.

FERC Federal Energy Regulatory Commission

Regulates the interstate transmission of electricity, natural gas, and oil.

FPC Federal Privacy Council

An interagency council that coordinates government-wide privacy initiatives.

GSA General Services Administration

Manages federal property and supports the basic functioning of federal agencies.

HHS Department of Health and Human Services

Protects the health of Americans and provides essential human services.

HUD Department of Housing and Urban Development

Supports community development and homeownership.

ISCP Interagency Council on Statistical Policy

Coordinates statistical work across federal agencies.

IRA Independent Regulatory Agencies

Agencies that operate independently of the executive branch.

NASA National Aeronautics and Space Administration

Responsible for the civilian space program and aeronautics research.

NCD National Cyber Director

Leads the development and implementation of national cyber policy and strategy.

NIFA National Institute of Food and Agriculture

Provides leadership and funding for agricultural research and extension programs.

NIST National Institute of Standards and Technology

Promotes innovation and industrial competitiveness through standards and technology.

NSF National Science Foundation

Supports fundamental research and education in science and engineering.

NTIA National Telecommunications and Information Administration

Advises the President on telecommunications and information policy issues.

OMB Office of Management and Budget

Oversees the administration's budget development and execution.

OPPRP Office of Pandemic Preparedness and Response Policy in the White House

Coordinates the federal government's pandemic preparedness and response efforts.

OPM Office of Personnel Management

Manages the civil service of the federal government.

OSTP Office of Science and Technology Policy

Advises the President on the effects of science and technology on domestic and international affairs.

PCAST President's Council of Advisors on Science and Technology

Advises the President on science, technology, and innovation policy.

SRMA Sector Risk Management Agency

Agencies responsible for managing risks to critical infrastructure sectors.

Treasury Department of the Treasury

Manages federal finances and collects taxes.

USAID United States Agency for International Development

Administers civilian foreign aid and development assistance.

USDA Department of Agriculture

Develops and executes federal laws related to farming, forestry, rural development, and food.

USDC United States Digital Corps

A two-year fellowship that recruits early-career technologists to serve in the federal government.

USDS United States Digital Service

Works across the federal government to modernize digital services.

USG NSS United States Government National Standards Strategy

A strategy for developing and using voluntary consensus standards in federal agencies.

USTPO United States Patent and Trademark Office

Grants patents and registers trademarks.

VA Department of Veterans Affairs

Provides healthcare and benefits to military veterans.