Algorithmic Foreign Policy and Executive Agreements: Reassessing Legal Accountability in the Age of Artificial Intelligence

Alvin Hoi-Chun Hung†

This Article examines the legal and constitutional implications of a significant yet underexplored development in U.S. foreign relations: the emergence of algorithmic foreign policy, where artificial intelligence (AI) systems are increasingly influencing or autonomously generating decisions traditionally reserved for human policymakers. From autonomous weapons systems to AI-enhanced surveillance pacts and predictive diplomacy tools, executive agreements now encode algorithmic logic into national security and foreign policy. The constitutional and legal frameworks that govern these executive agreements remain rooted in assumptions of human discretion, deliberative process, and political accountability. This study argues that existing doctrines, including the *political question doctrine* and the *War Powers Resolution*, are ill-equipped to regulate AI-infused foreign relations. It offers an innovative framework for algorithmic legal accountability, reconciling emerging AI capabilities with the principles of separation of powers, treaty processes, and transparency norms. Drawing on case studies involving autonomous drone strikes, cyber operations, and AI-led diplomatic communications, this Article identifies doctrinal gaps and proposes legal reforms to ensure that AI-augmented executive agreements remain constitutionally constrained, democratically legitimate, and subject to judicial review.

† Assistant Professor, School of Law, City University of Hong Kong. DPhil, University of Oxford; LL.M., London School of Economics and Political Science. Solicitor (Hong Kong).

Introduction

In June 2025, the United States conducted precision airstrikes, codenamed "Operation Midnight Hammer", against three Iranian nuclear facilities at Fordow, Natanz, and Isfahan.[1] According to the Pentagon, the strikes began in the early morning hours of June 22, 2025, involving several B-2 stealth bombers dropping fourteen GBU-57 bunker-buster bombs, alongside submarine-launched Tomahawk missiles.[2] The operation drew scrutiny from Congress, with critics warning it violated the War Powers Resolution[3] and bypassed legislated authorization.[4]

---

1. *See, e.g.*, Natasha Bertrand, Katie Bo Lillis & Zachary Cohen, *Early US Intel Assessment Suggests Strikes on Iran Did Not Destroy Nuclear Sites, Sources Say*, CNN, (June 25, 2025), https://edition.cnn.com/2025/06/24/politics/intel-assessment-us-strikes-iran-nuclear-sites [https://perma.cc/DE63-UK4S]. *See also* David Albright, Sarah Burkhard, Spencer Faragasso, & the Good ISIS Team, *Comprehensive Updated Assessment of Iranian Nuclear Sites Five Months After the 12-Day War*, Inst. for Sci. & Int'l Sec., Nov. 21, 2025, https://isis-online.org/isis-reports/comprehensive-updated-assessment-of-iranian-nuclear-sites-five-months-after-the-12-day-war [https://perma.cc/EYQ5-A8KC]. "Operation Midnight Hammer" was the codename for the United States' decisive June 2025 covert airstrikes, which precision-targeted Iran's critical nuclear facilities at Fordow, Natanz, and Isfahan. Each of these three places serves a different, specialized function within Iran's nuclear program. Fordow is a deeply-buried uranium enrichment site, Natanz is Iran's main large-scale enrichment facility with extensive underground halls, and Isfahan is a nuclear technology center for uranium conversion and fuel fabrication.

2. David Vergun, *Defense Agency Contributed Toward Operation Midnight Hammer Success*, U.S. Dep't of War (July 10, 2025), https://www.defense.gov/News/News-Stories/Article/Article/4240876/defense-agency-contributed-toward-operation-midnight-hammer-success/ [https://perma.cc/A6VJ-VZAX].

3. *See* War Powers Resolution, 50 U.S.C. §§ 1541–1548 (1973). The War Powers Resolution asserts Congress's authority over the use of U.S. armed forces by requiring the President to notify Congress within 48 hours of committing troops, and mandates their withdrawal within sixty days unless Congress authorizes continued military action.

4. *See* Farrah Tomazin, *Top General Immediately Undercuts Pete Hegseth's Claim Iran Was a 'Massive Success'*, The Daily Beast (June 27, 2025), https://www.thedailybeast.

As the debate over the legality of the strikes intensified, attention shifted to the technologies that underpinned the operation. An even more significant issue emerged: the use of advanced artificial intelligence (AI) modeling throughout *Operation Midnight Hammer*.[5] National security officials acknowledged the importance of leveraging AI capabilities.[6] However, AI-driven systems did not directly influence the targeting decisions themselves.[7] Operated within parameters set by executive mandate, these AI algorithms introduced new complexities regarding the opacity of decision-making, the adequacy of existing oversight mechanisms, and the risk of further insulating lethal operations from democratic accountability.[8] The growing reliance on AI tools, even in outcome analysis rather than targeting, signals a profound shift in how accountability and transparency must be addressed in modern national security operations.[9]

While past controversies, most notably the 2020 drone strike that killed Qasem Soleimani,[10] focused on human actors issuing orders, the 2025 strikes signal a transformation of how autonomous or semi-autonomous AI systems could soon determine targets, operating under executive agreements outside the reach of Congress or public scrutiny.[11] As algorithmic decision-making penetrates national security, surveillance, and diplomatic operations, the gap between speculative fiction and reality narrows, and the legal frameworks for accountability must evolve accordingly.

This Article identifies and examines a novel yet critical development at the intersection of foreign relations law and emerging technologies: algorithmic foreign policy, which involves the integration of AI systems into processes traditionally dominated by human discretion and political accountability. Drawing upon interdisciplinary insights from constitutional law, national security policy, and emerging technology studies, this Article offers a systematic

---

com/top-general-immediately-undercuts-pete-hegseths-claim-iran-was-a-massive-success [https://perma.cc/5XV8-Q69U].

5. *See* Andrew Roth, *Hegseth Defends Iran Strike Amid Doubts Over Trump's 'Obliteration' Claims*, The Guardian (June 27, 2025), https://www.theguardian.com/us-news/2025/jun/26/hegseth-iran-nuclear-strike-intel [https://perma.cc/U76B-TD5Y].

6. "Transcript: Senior Defense Officials Discuss the Iran Nuclear Facilities Bombing," U.S. Dep't of War (July 10, 2025), https://www.war.gov/News/Transcripts/Transcript/Article/4242273/senior-defense-officials-discuss-the-iran-nuclear-facilities-bombing/ [https://perma.cc/5BK3-TPNW].

7. *Id.*; "Beyond the Buzz: 3 Ways AI Transforms Command and Control," Virtualitics, https://virtualitics.com/beyond-the-buzz-3-ways-ai-transforms-command-and-control/ [https://perma.cc/L58V-B4F2] (last visited Jan. 15, 2026).

8. For a review of how these AI algorithms raised concerns about secrecy, weak oversight, and diminished accountability, *see* Madalina Busuioc, *AI Algorithmic Oversight: New Frontiers in Regulation*, *in* Handbook of Regulatory Authorities 470-480 (Edward Elgar, 2022).

9. *Id.* at 481-82.

10. Luca Ferro, *Killing Qasem Soleimani: International Lawyers Divided and Conquered*, 53 Case W. Res. J. of Int'l L. 163, 170–76 (2021) (analyzing the Soleimani strike as an instance of executive-directed lethal targeting conducted without meaningful congressional oversight).

11. *See* Bertrand, *supra* note 1; *see* Vergun, *supra* note 2. *See generally* H. Akin Ünver, Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation, Econ. & Foreign Policy Ctr. (EDAM) Res. Rep.: Cyber Governance and Digital Democracy No. 3, at 7–10, 15–18, 21–22 (2017) (describing how algorithmic tools in foreign policy reduce transparency and create structural barriers to congressional and public oversight).

examination of the constitutional implications of algorithmic foreign policy. It critically assesses how existing doctrines, from the nondelegation principle to the War Powers Resolution,[12] falter when confronted with AI-driven executive agreements.[13] Recognizing this vulnerability, the Article proposes a novel framework of algorithmic legal accountability. This framework seeks to ensure democratic legitimacy, constitutional compliance, and judicial reviewability, even as AI technologies become integral to the United States' international engagements.

Beginning with an overview of the executive agreement's evolving legal framework, this Article explores how algorithmic technologies are reshaping national security decision-making and introduces the concept of algorithmic foreign policy. The discussion then turns to the constitutional tensions and doctrinal uncertainties triggered by these developments, including issues of accountability, judicial review, the erosion of human judgment, and the complexities of war powers in an AI-driven environment. Building on these analyses, the Article presents a normative and comparative framework for legal accountability. Then, it illustrates the stakes through detailed case studies on autonomous weapons, surveillance, and AI-facilitated diplomacy. The final sections propose concrete steps for constructing a legally responsible algorithmic state, identifying constitutional thresholds, and outlining pathways for legislative and executive reform.

I. Executive Agreements and Algorithmic Tools

The intersection of foreign relations law and AI is rapidly redrawing the boundaries of executive power and statecraft.[14] To understand the implications of algorithmic governance, it is first necessary to map the evolving terrain of executive agreements, such as their legal foundations, forms, and doctrinal contours, and to examine the proliferation of algorithmic tools now deployed in diplomacy, national security, and intelligence operations. This section situates executive agreements within their constitutional and jurisprudential context, traces the emergence of predictive analytics and autonomous systems in foreign policy decision-making, and introduces the concept of algorithmic foreign policy. By charting both the doctrinal landscape and the technological innovations shaping contemporary practice, the analysis lays the groundwork

12. Stephen L. Carter, *The Constitutionality of the War Powers Resolution*, 70 Va. L. Rev. 101, 103–08 (1984) (analyzing the structural limits Congress attempted to place on unilateral presidential uses of force and explaining why the Resolution's constraints remain doctrinally fragile).

13. *See*, *e.g.,* Curtis Bradley & Jack Goldsmith, *Foreign Affairs, Nondelegation, and the Major Questions Doctrine*, 172 U. Pa. L. Rev. 1743, 1758–67 (2023) (arguing that foreign-affairs delegations, including those enabling executive agreements, receive unusually deferential judicial review and illustrating how broad discretion in this domain raises renewed nondelegation concerns).

14. Sertaç Canalp Korkmaz, *Emerging Technologies and Power Asymmetry in International System: An Analysis over Artificial Intelligence*, *in* Artificial Intelligence 84, 88–90 (Utku Kose & Mustafa Umut Demirezen, eds., 2024) (explaining how AI-enabled capabilities reshape strategic decision-making and alter the distribution of power among states).

for evaluating how legal and institutional structures must adapt in response to the algorithmic turn in American foreign relations.

A. The Legal Landscape of Executive Agreements

Executive agreements occupy a constitutionally recognized, yet doctrinally contested, space within United States foreign relations law.[15] Unlike Article II treaties,[16] which require the advice and consent of two-thirds of the Senate, executive agreements can be concluded without such legislative ratification.[17] These instruments have proliferated in the modern administrative state, offering presidents a mechanism to engage in binding international commitments while circumventing traditional treaty procedures.[18] A clear understanding of the different forms of executive agreements, such as treaties, sole executive agreements, and congressional-executive agreements, is essential before considering how algorithmic systems may alter or complicate their legal structure.

Treaties remain the most formal type of international agreement under U.S. law, as specified in Article II, Section 2 of the Constitution.[19] They require Senate approval and have been increasingly reserved for high-stakes multilateral arrangements. Sole executive agreements, by contrast, are made by the President acting alone, based either on inherent constitutional authority or on prior statutory delegation.[20] Congressional-executive agreements involve a statutory framework, wherein both houses of Congress pass legislation that either authorizes or approves a specific international commitment.[21] Though often functionally equivalent to treaties in terms of binding effect, they raise distinct constitutional questions regarding the scope of legislative delegation and presidential discretion.[22]

The Supreme Court has not offered a definitive taxonomy of executive agreements, but its jurisprudence provides essential guidance.[23] In *United States*

---

15. John C. Yoo, *Laws as Treaties?: The Constitutionality of Congressional-Executive Agreements*, 99.4 Mich. L. Rev. 757, 759-760 (2001) (describing the constitutional basis and ongoing scholarly dispute over the legitimacy and limits of congressional–executive agreements).

16. *See* U.S. Const. art. II, § 2, cl. 2. The U.S. Constitution authorizes the President to make treaties (with Senate consent) and recognizes the President's foreign relations powers.

17. Andrew Kent, Ethan J. Leib & Jed Handelsman Shugerman, *Faithful Execution and Article II*, 132 Harv. L. Rev. 2111, 2149–55 (2019) (discussing the constitutional limits of presidential authority and distinguishing the treaty-making process requiring Senate consent from executive agreements that may be concluded without such approval).

18. *Id.* at 2149-54.

19. *See* Peter E. Quint, *What Is a Twentieth-Century Constitution?*, 67 Md. L. Rev. 238 (2007) (discussing the heightened formality of Article II treaty-making and explaining why the Constitution treats treaties as the most formal type of international agreement).

20. *See* John K. Setear, *The President's Rational Choice of a Treaty's Preratification Pathway: Article II, Congressional-Executive Agreement, or Executive Agreement?*, 31 J. Legal Stud. S5, S12–S14 (2002) (explaining that sole executive agreements rest on either independent presidential authority or statutory delegation).

21. Curtis A. Bradley, *Exiting Congressional-Executive Agreements*, 67 Duke L.J. 1615, 1625 (2018) (describing congressional-executive agreements as dependent on legislation passed by both houses authorizing or approving the international commitment).

22. *Id.* at 1615-1617.

23. *See* Peter J. Spiro, *Treaties, Executive Agreements, and Constitutional Method*, 79 Tex. L. Rev. 961, 972–74 (2001) (noting that the Court has not provided a comprehensive taxonomy of executive agreements but that its decisions nonetheless shape their constitutional status).

v. Curtiss-Wright Export Corp.,[24] the Court articulated an expansive vision of presidential authority in foreign affairs, emphasizing that the President is supposed to be the sole organ of the federal government in the field of international relations.[25] Although this dictum has been the subject of sustained academic critique, it remains foundational to arguments in favor of broad unilateral executive power in foreign engagements.[26] In *United States v. Pink*,[27] the Court reaffirms the authority of executive agreements to preempt state law.[28] Later decisions placed limits on this power. In *Zivotofsky v. Kerry*,[29] the Court reaffirmed the President's exclusive power to recognize foreign states, striking down a statute that sought to require listing "Israel" as the place of birth on passports for U.S. citizens born in Jerusalem.[30] The ruling underscored the President's primacy in certain diplomatic functions but did not sanction a blanket authority to enter into all forms of international commitments without congressional input.[31] Similarly, in *Dames & Moore v. Regan*,[32] the Court upheld an executive agreement resolving the Iran hostage crisis, reasoning that Congress had implicitly approved of such actions through related statutory frameworks.[33] The Court adopted a functionalist and pragmatic approach, grounding the validity of executive agreements in a combination of historical practice and legislative acquiescence.[34] This case illustrates the judiciary's willingness to tolerate flexible arrangements in the realm of national security, especially during exigent circumstances.

---

24. *United States v. Curtiss-Wright Exp. Corp.,* 299 U.S. 304 (1936).

25. *See* Charles A. Lofgren, *United States v. Curtiss-Wright Export Corporation: An Historical Reassessment*, 83 Yale L. J. 1, 4 (1973) (discussing the Court's adoption of the "sole organ" conception of presidential authority in foreign affairs).

26. Saikrishna B. Prakash & Michael D. Ramsey, *The Executive Power over Foreign Affa*irs, 111 Yale L.J. 231, 248–52 (2001) (critiquing the historical basis of the "sole organ" dictum while noting its continued prominence in arguments favoring broad presidential power. The "sole organ" is a conception of the President's exclusive and plenary authority to act as the representative of the United States in its international relations and to articulate foreign policy).

27. *United States v. Pink*, 315 U.S. 203 (1942).

28. Justice Roberts, *United States v. Pink*. 36.2 Am. J. Int'l L. 309-338 (1942) (providing contemporaneous scholarly analysis of the Court's reaffirmation that executive agreements may preempt state law and explaining the decision's significance for theories of broad presidential foreign-affairs authority).

29. *Zivotofsky v. Kerry*, 576 U.S. 1 (2015).

30. Hannah Cole-Chu, *Zivotofsky v. Kerry: Choosing International Reputation over Separation of Powers*, 75 Md. L. Rev. 865, 868–71 (2016) (summarizing the Court's reasoning that the passport-designation statute unconstitutionally interfered with the President's exclusive recognition power).

31. *Id.* at 868-70.

32. *Dames & Moore v. Regan*, 453 U.S. 654 (1981). The case upholds the President's authority to settle claims with foreign governments via executive agreements, particularly in the context of emergencies.

33. *See* Arthur S. Miller, *Dames & Moore v. Regan: A Political Decision by a Political Court*, 29 UCLA L. Rev. 1104, 1110–13 (1982) (describing the Court's reliance on implicit congressional authorization, including IEEPA, in upholding the executive agreement resolving the hostage crisis).

34. *See* Louis D. Montressor, *Dames & Moore v. Regan*, 3 J. Int'l & Comp. L. 73, 76–78 (1981) (describing the Court's functional reliance on historical practice and congressional acquiescence in upholding the executive agreement).

These precedents collectively reveal that the legitimacy of executive agreements is not a function of rigid constitutional categories, but of context-specific interactions between the executive and legislative branches. As AI tools become embedded in the formulation, implementation, and even generation of such agreements, the established legal framework may prove inadequate.[35] The question now extends beyond whether an executive agreement conforms to an accepted constitutional form. It must address whether algorithmically generated or mediated actions, operating under the guise of executive discretion, can be reconciled with foundational principles of democratic accountability and legal oversight.[36]

B. The Rise of Algorithmic Instruments in National Security

The *National Security Act* establishes the foundational legal framework governing intelligence activities and their oversight.[37] In recent years, the architecture of national security has been shaped not only by diplomatic judgment and military doctrine, but also by the growing influence of algorithmic computation.[38] AI now occupies a central role in American foreign policy, ranging from predictive models that forecast geopolitical developments to autonomous systems deployed in surveillance and cyber operations.[39] The *Foreign Intelligence Surveillance Act*[40] sets forth procedures for electronic surveillance and the collection of foreign intelligence, with significant implications for algorithmic data analysis and AI-driven monitoring.[41] As algorithmic systems increasingly move from supporting executive decision-making to driving it, a fundamental reconfiguration of executive functions is underway.[42] This

35. Patricia Gomes Rêgo de Almeida, Carlos Denner dos Santos, and Josivania Silva Farias, *Artificial Intelligence Regulation: A Framework for Governance*, 23.3 Ethics & Info. Tech. 505, 506-508 (2021) (explaining that the integration of AI into governmental and policy processes exposes gaps and inadequacies in existing legal and governance structures).

36. Daniel J. Bogiatzis-Gibbons, *Beyond Individual Accountability: (Re-)Asserting Democratic Control of AI*, *in* Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency 74, 75–77 (2024) (explaining how algorithmic systems can obscure responsibility and undermine traditional mechanisms of democratic and legal accountability).

37. National Security Act of 1947, Pub. L. No. 80-253, §2, 61 Stat. 495 (codified as amended in sections 5 & 50 U.S.C.).

38. Ben Scott, Stefan Heumann & Philippe Lorenz, *Artificial Intelligence and Foreign Policy*, Stiftung Neue Verantwortung Policy Brief 3–5 (January 2018) (explaining how AI and computational analytics are reshaping intelligence practices, strategic planning, and foreign-policy decision-making).

39. Jake Sullivan, *The Sources of American Power: A Foreign Policy for a Changed World*, Foreign Aff. (Oct. 24, 2023), https://www.foreignaffairs.com/united-states/sources-american-power-biden-jake-sullivan [https://perma.cc/T4YG-Y5DD] (describing AI-driven intelligence, predictive analytics, and autonomous systems as central elements of contemporary U.S. foreign policy and national power).

40. *Foreign Intelligence Surveillance Act* (FISA), 50 U.S.C. § 1801-1811 (1994 & Supp. 1999).

41. *See* Barbara Ann Stolz, *The Foreign Intelligence Surveillance Act of 1978: The Role of Symbolic Politics*, 24 Law & Pol'y 269, 272–76 (2002) (describing FISA's procedural requirements for electronic surveillance and its regulatory structure for foreign-intelligence collection).

42. Mary L. Cummings, et al., *Artificial Intelligence and International Affairs* 7-18 (Chatham House, 2018) (describing how AI systems increasingly structure and, in some cases, determine foreign-policy and national-security decision processes).

transformation raises critical questions concerning the delegation of authority, accountability mechanisms, and the constitutional structure underlying U.S. foreign relations law.

Predictive analytics now play an integral role in identifying patterns of international instability, forecasting conflict zones, and modeling adversarial behavior.[43] These tools draw from large-scale, often unstructured datasets (ranging from open-source intelligence to satellite imaging) to generate risk assessments that shape State Department planning and Department of Defense posturing.[44] For example, AI-enabled platforms developed under the Joint AI Center (JAIC) have been tasked with anticipating resource-based conflicts and disinformation threats in strategically sensitive regions.[45] These systems are increasingly used to recommend allocations of diplomatic capital or force projection, effectively influencing the calculus behind foreign commitments and executive agreements.[46]

While such tools promise efficiency and foresight, they also obscure the locus of responsibility. In traditional legal frameworks, the President and designated officers are held accountable for foreign engagements.[47] When algorithmic models suggest courses of action based on opaque inputs and machine-trained correlations, the human agents responsible for oversight may not fully understand, much less interrogate, the rationale behind the recommended diplomatic strategies.[48] This risks displacing not only legal accountability but also the deliberative process essential to the governance of foreign relations.

Autonomous and semi-autonomous systems, ranging from drone-based reconnaissance to algorithmically guided cyber-intrusion tools, further

---

43. *See, e.g.*, Pedro Manuel Sequeira Estrela Moleirinho, *The Era of Predictive Models: Between Risks and Unstable Balance*, *in* Security at a Crossroad: New Tools for New Challenges 95, 95–101 (Nova Sci. Publishers, 2019) (examining how predictive-analytics tools assess instability, forecast conflict trajectories, and model adversarial behavior for security planning purposes).

44. James Johnson, *Artificial Intelligence & Future Warfare: Implications for International Security*, 35.2 Def. & Sec. Analysis 147, 152–55 (2019) (describing how AI systems synthesize large, unstructured datasets—including OSINT and satellite imagery—to produce risk assessments that guide military and strategic planning).

45. Yasmin Tadjdeh, *Joint Artificial Intelligence Center Keeps Branching Out*, Nat'l Def. (Nov. 3, 2020), https://www.nationaldefensemagazine.org/articles/2020/11/3/joint-artificial-intelligence-center-keeps-branching-out [https://perma.cc/576T-3SB8] (describing JAIC initiatives that use AI systems to assess instability, anticipate emerging threats, and support defense-planning functions).

46. *See, e.g.*, Seyed-Ali Sadegh-Zadeh, *Dynamics of Global Trade Diplomacy: An Artificial Intelligence Multi-Dimensional Analysis of Preferential Trade Agreements*, 8 J. of Computational Soc. Sci. 63, 70–72 (2025) (explaining how AI-based multidimensional trade-diplomacy models generate recommendations for states' diplomatic resource allocation and treaty-making strategies).

47. *See* H. Jefferson Powell, *President's Authority over Foreign Affairs: An Executive Branch Perspective*, 67 Geo. Wash. L. Rev. 527, 531–34 (1998) (describing how U.S. foreign-affairs law places responsibility for international commitments on the President and identifiable executive officers).

48. *See generally* Veronika Solopova, Hybrid AI Systems in Automated Content Moderation and Analysis (2024) (Ph.D. dissertation, Freie Universitaet Berlin, Germany). Refer to pp. 112–18 (describing how hybrid AI systems rely on opaque data correlations and produce outputs that human reviewers often cannot fully interpret or audit).

complicate the executive's national security apparatus.[49] These technologies operate in environments that are temporally compressed and legally opaque, such as real-time cyber engagements where attribution and proportionality remain elusive. AI tools deployed through the National Security Agency (NSA), U.S. Cyber Command, and allied partners are increasingly acting on pre-authorized decision protocols.[50] These tools raise the possibility that foreign actions with diplomatic consequences, such as violations of sovereignty or unintended escalation, may occur without direct, contemporaneous human authorization.[51]

Notably, AI systems can shape foreign policy in practice even without formal instruments.[52] An AI-guided surveillance regime focused on foreign diplomatic missions, for instance, may alter the tenor of bilateral relations.[53] Yet, these systems typically operate within classified domains, outside the scrutiny of Congress or the judiciary.[54] The displacement of human oversight in such contexts destabilizes the assumption, rooted in *United States v. Curtiss-Wright Export Corp.* and reinforced in *Zivotofsky v. Kerry,* that identifiable, accountable actors exercise foreign relations authority within a constitutional hierarchy.[55]

Beyond operational systems, executive agencies have begun experimenting with AI in core diplomatic functions: drafting cable communications, prioritizing foreign aid allocations, and even generating language for use in informal understandings or memoranda of cooperation.[56] Large language models (LLMs), such as OpenAI's GPT-based tools or government-trained equivalents,

---

49. My Abdelmajid Kassem, et al. *Advancing AI, ML, and Bioinformatics for Transformative Research Across Disciplines*, J. A.I., Mach. Learning, & Bioinformatics 1, 4–7 (2024) (describing how AI-enabled autonomous and semi-autonomous systems support reconnaissance, data-driven targeting, and cyber-analytic operations).

50. *See, e.g.,* Esther Chinwe Eze et al., *The role of AI in National Cybersecurity Policy and Resilience Planning: A Comprehensive Analysis of the United States' Strategic Approach,* 27 World J. Advanced Res. & Rev. 1381, 1382–84 (2025) (describing how U.S. national-security agencies have begun integrating AI for automated threat detection, response automation, and resilience planning in cyber defense).

51. *See, e.g.*, National Security Commission on Artificial Intelligence, Final Report 82–86 (Mar. 5, 2021), , https://apps.dtic.mil/sti/html/trecms/AD1124333/ [https://perma.cc/79U6-4WSB] (warning that AI-enabled military and intelligence systems may act autonomously at machine speed, creating risks of unintended escalation and sovereignty-implicating actions without real-time human authorization).

52. Paul A. Anderson and Stuart J. Thorson, *Systems Simulation Artificial Intelligence Based Simulations of Foreign Policy Decision Making*, 27 Behav. Sci. 176, 178–80 (1982) (explaining how AI-based simulations influence policymakers' threat assessments and strategic choices even in the absence of formal diplomatic instruments).

53. Kwadwo Osei Bonsu and Jie Song, *Turbulence on the Global Economy Influenced by Artificial Intelligence and Foreign Policy Inefficiencies*, 6 J. Liberty & Int'l Affs 113, 120–23 (2020) (explaining how AI-enhanced surveillance and monitoring practices can heighten diplomatic tension and negatively affect bilateral relations).

54. *Id.* at 114-120.

55. David A. Lake, *Hierarchy in International Relations: Authority, Sovereignty, and the New Structure of World Politics 6–9* (Ann. Meeting of the Am. Pol. Sci. Ass'n, 2004) (arguing that authority in international relations depends on identifiable decisionmakers within hierarchical structures, and explaining how diffusion of agency undermines accountability).

56. *See* Syed Shah Hussain, *Artificial Intelligence and Diplomacy: Transforming International Relations in the Digital Age*. 9 Remittances Rev. 988, 992–95 (2024) (detailing how foreign-affairs institutions use AI to draft diplomatic communications, structure aid-allocation decisions, and generate language for informal diplomatic instruments).

are used to compose initial drafts of interagency communiqués or identify patterns across foreign correspondence.[57] The National Geospatial-Intelligence Agency and other intelligence community agencies have integrated natural language processing to streamline the analysis of foreign media, sometimes with minimal post-algorithmic human review.[58]

This delegation raises novel concerns regarding executive agreements, particularly when language generated or prioritized by AI systems serves as the substantive basis for negotiation or representation.[59] The constitutional legitimacy and oversight of AI-generated agreements are questionable if the AI's output is influenced by bias or lacks transparency.[60] Such situations undermine both the process of executive foreign engagement and the knowledge base essential for legal accountability.[61]

As AI systems assume roles of increasing influence in national security and diplomacy, the traditional assumptions underlying executive foreign relations powers are strained.[62] Algorithmic tools increasingly obscure the distinction between advice and decision-making, as well as between support and substitution.[63] When legal responsibility is distributed across machine-driven processes, executive agreements must be reconsidered, not just as formal legal acts, but as products of complex and often opaque computational systems.[64]

---

57. Muhammad Usman Hadi et al., *Large Language Models: A Comprehensive Survey of its Applications, Challenges*, 1 TechRxiv 14–18 (2023) (describing LLM capacities for generating draft text, summarizing extensive document sets, and extracting patterns across large collections of communications).

58. *See, e.g.*, Jeffry A. Coady, et al., *Development of a Cognitive Assessment System for Evaluating Geospatial Intelligence Analysis*, *in* Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications VII, 6–9 (2025) (describing the integration of NLP systems into geospatial-intelligence workflows, including automated extraction and analysis of foreign-language media with limited human review).

59. *See* Theodore Christakis, *Data Free Flow with Trust: Current Landscape, Challenges and Opportunities*. 9 J. Cyber Pol'y 95, 101–04 (2024) (discussing how automated and AI-supported drafting practices influence the substance of cross-border data governance instruments and raise legitimacy concerns).

60. Alex Whaples, *AI Regulation Across Borders: Legal Challenges and Prospects for International Cooperation*, 26 San Diego Int'l L.J 317, 330–34 (2025) (discussing how bias and opacity in AI systems undermine transparency, accountability, and the legitimacy of cross-border legal or diplomatic decision-making).

61. *See generally* Susan Rose-Ackerman, *Democracy and Executive Power: Policymaking Accountability in the US, the UK, Germany, and France* 45–72, 115–38 (Yale Univ. Press 2021) (examining how democratic systems require transparency, reviewability, and reason-giving in executive decision-making, principles that illuminate why opaque or biased AI-generated agreements threaten constitutional accountability).

62. *See generally* Marta Konovalova, *AI and Diplomacy: Challenges and Opportunities*. 9 J. Liberty & Int'l Aff. 520, 526–29 (2023) (discussing how AI's growing role in diplomacy and security decision-making disrupts traditional assumptions about human-centered foreign-relations authority).

63. Andrej Gill et al., *Dynamics of Reliance on Algorithmic Advice*, 37 J. Behav. Decision Making e2414, e2414–e2416 (2024) (showing that reliance on algorithmic recommendations can shift from consultation to de facto substitution, blurring the boundary between advice and decision-making).

64. *See generally* Curtis A. Bradley et al., *The Rise of Nonbinding International Agreements: An Empirical, Comparative, and Normative Analysis*, 90 U. Chi. L. Rev. 1281, 1290–94 (2023) (explaining that modern international agreements increasingly emerge from diffuse, bureaucratic processes that complicate attribution of responsibility and challenge traditional assumptions about executive control).

Acknowledging this transformation is crucial for developing a legal framework that remains consistent with both constitutional principles and technological advancements.

C. Conceptualizing Algorithmic Foreign Policy

AI is no longer merely an operational tool within U.S. foreign policy; it is becoming a site of policy itself.[65] The emergence of what may be termed *algorithmic foreign policy* reflects a structural shift in how diplomatic authority is exercised, institutionalized, and mediated by computational systems.[66] Whereas executive power in foreign affairs was traditionally conceptualized as resting in identifiable human actors, subject to political and constitutional constraints, the introduction of AI into foreign relations challenges both the locus of authority and the mechanisms of legal accountability.[67] To conceptualize algorithmic foreign policy, one must grapple with its definitional scope, the typologies of machine delegation, and the layered structure of government actors entangled in its design, implementation, and oversight.[68]

The concept of algorithmic foreign policy refers to the integration of AI systems, including machine learning models, large language models (LLMs), autonomous agents, and rule-based decision-making architectures, into the formulation, execution, and sometimes expression of the United States' external relations.[69] This includes not only operational tools, such as predictive targeting software, but also epistemic instruments that filter, prioritize, or generate the content of diplomatic knowledge and representation.[70] What distinguishes algorithmic foreign policy from conventional digitized governance is the degree to which AI systems influence or supplant core functions that have

65. Jascha Bareis & Christian Katzenbach, *Talking AI Into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics*, 47 Sci. Tech. & Hum. Values 855, 860–64 (2022) (explaining that national AI strategies frame AI as a domain of governance and political action, not merely as a technological tool).

66. *See, e.g.*, Alexander Belosludtsev & Elena Dziuba, *Generative Artificial Intelligence in the System of International Relations: Risks Opportunities, and Regulations*, *in* Proceedings of Topical Issues in International Political Geography 187, 190–93 (2024) (discussing how generative AI reshapes diplomatic processes, mediates state interactions, and transforms institutional structures in international relations).

67. *See generally* Bhaso Ndzendze & Tshilidzi Marwala. *Artificial Intelligence and International Relations Theories* 33 (Palgrave Macmillan, 2023). In particular, *see* 33–54 (explaining how AI alters the distribution of agency and authority in international relations, undermining traditional assumptions about human-centered decision-making and accountability).

68. *Id.* at 33-56.

69. Bert Chapman, *How U.S. Government Policy Documents Are Addressing the Increasing National Security Implications of Artificial Intelligence*, 11 J. Advanced Mil. Stud. 209, 214–18 (2020) (reviewing U.S. national-security policy documents that describe the integration of machine-learning models, autonomous systems, and other AI tools into foreign-policy and national-security processes).

70. *See, e.g.*, Christian Bueger, *Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy*, 9 Int'l pol. sociology 1, 4–7 (2015) (demonstrating how epistemic practices within international institutions filter, translate, and produce knowledge that shapes diplomatic understanding and representation).

historically been reserved for elected or appointed officials: judgment, discretion, and interpretation.[71]

In practice, this conceptual frame encompasses a spectrum of AI-mediated conduct, ranging from internal threat assessments that inform executive agreements with foreign powers, to language generated by LLMs that drafts preliminary diplomatic memoranda, to real-time systems that trigger cross-border cyber operations without direct human oversight.[72] The key inquiry is not whether such outputs are formally denominated agreements, but whether they functionally instantiate positions, obligations, or expectations in the domain of foreign affairs.[73] Algorithmic foreign policy does not operate on a single mode of delegation. Rather, it unfolds along a continuum of machine involvement that corresponds to different legal and constitutional implications, including assisted, augmented, and autonomous intelligence systems.[74]

Assisted intelligence systems provide information or analytics that support human decision-making but do not direct it.[75] An example would be a threat matrix that informs embassy staffing decisions or sanctions designations. These systems raise fewer normative concerns, though questions remain about transparency and model bias. *Augmented intelligence systems* do more than assist; they filter or prioritize options based on algorithmic logic, effectively narrowing the scope of human discretion.[76] For instance, an LLM that ranks treaty clauses or recommends language based on prior agreements might materially shape the negotiation process.[77] The risk here is epistemic capture, where human actors defer to computational reasoning without a full understand-

71. *See generally* H. Akın Ünver, *Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation*, EDAM Research Reps., Cyber Governance and Digital Democracy 3, 9–12 (2017) (explaining how algorithmic tools shape and sometimes replace human judgment, discretion, and interpretive functions in diplomatic communication and decision-making).

72. *See* Anton Michael Pillay, *Artificial Intelligence's (AI) Pro-US Foreign Policy Stance – A New Global Security Challenge*, 10 NETSOL: New Trends Soc. & Liberal Sci. 1, 7–8, 10–11, 13–14 (2025) (pages 7–8 discussing AI-generated threat assessments used in foreign-policy decision-making; pages 10–11 analyzing language-generation systems that produce draft diplomatic text; pages 13–14 examining automated or semi-autonomous cyber operations with minimal human supervision).

73. *See generally* Ben Buchanan & Andrew Imbrie, *The New Fire: War, Peace, and Democracy in the Age of AI* 33-58 (MIT Press 2024) (explaining how AI-generated outputs can shape expectations, commitments, and strategic behavior among states even without taking the form of formal legal agreements).

74. *See Assisted, Augmented, and Autonomous Intelligence: What Differences?,* Dirox Studio (Feb. 16, 2023), https://dirox.com/post/assisted-augmented-and-autonomous-intelligence-what-differences [https://perma.cc/2C6F-2W74] (defining assisted, augmented, and autonomous intelligence systems and explaining the progressive levels of machine involvement that structure human–machine delegation).

75. *See* Abhinandan Singh Dandotiya et al., AI in Everyday Life: Transforming Society 12-19 (Navi International Book Publication House 2024) (defining "assisted intelligence" as systems that supply information or analytics to human users while leaving decision-making authority entirely with humans).

76. *See Nick* Lüthi et al., *Augmented Intelligence, Augmented Responsibility?* 65 Bus. & Info. Sys. Eng'g. 391, 395–98 (2023) (explaining how augmented-intelligence systems filter and prioritize options using opaque algorithmic logics, thereby limiting the range of choices available to human decisionmakers).

77. Johannes Loevenich et al., *Design and Evaluation of an Autonomous Cyber Defence Agent Using DRL and an Augmented LLM*, 262 Comput. Networks 111162, 111165–67 (2025)

ing of its premises.[78] *Autonomous intelligence systems* act with minimal or no real-time human oversight.[79] These include AI-enabled cyber tools that respond to perceived intrusions or surveillance algorithms that autonomously assign diplomatic threat levels. In such contexts, the boundaries between algorithmic behavior and executive action collapse, raising foundational questions about attribution, consent, and accountability.[80]

This typology of intelligence systems is not merely descriptive; it is legally operative.[81] The constitutional permissibility of delegating foreign affairs functions depends on whether the function is discretionary, whether Congress has authorized the delegation, and whether judicial review is available.[82] The further one moves along the spectrum toward autonomy, the more attenuated these legal safeguards become.

Algorithmic foreign policy is not monolithic; it is produced through overlapping layers of governmental actors and institutional logics.[83] At the front end, executive agencies such as the Department of Defense, State Department, and intelligence community serve as procurers and implementers of AI systems.[84] Contractors and private vendors, particularly those with longstanding ties to national security infrastructure (e.g., Palantir, Booz Allen Hamilton), frequently design the algorithms and shape their parameters.[85]

(demonstrating how augmented LLM systems use prior patterns to generate and rank recommended actions, influencing downstream human decision-making).

78. *See* Suriya Ganesh Ayyamperumal & Limin Ge, *Current State of LLM Risks and AI Guardrails* 3 (Jun. 16, 2024) (unpublished manuscript), https://arxiv.org/abs/2406.12934 [https://perma.cc/PFA7-T826]. Refer to, in particular, pages 3–5, explaining how automation bias and over-reliance on opaque LLM reasoning can lead human users to defer to model outputs without understanding their assumptions.

79. *See* Jie Chen, Jian Sun & Gang Wang, *From Unmanned Systems to Autonomous Intelligent Systems*,12 Eng'g 16, 17, 17-18 (2022) (defining autonomous intelligent systems as those capable of independent perception and decision-making, operating with minimal or no real-time human control).

80. *See* Jonas Lundberg & Björn J.E. Johansson, *A Framework for Describing Interaction Between Human Operators and Autonomous, Automated, and Manual Control Systems*, 23 Cognition, Tech. & Work 381, 384–87 (2021) (explaining how increasing system autonomy blurs the line between machine-initiated and human-directed actions, complicating attribution and responsibility).

81. *See generally* Alexander Morningstar, *Distinguishing Between Operational and Intelligence Activities: A Legal Framework*, 2022 Army L. 63, 70–73 (2022) (explaining that distinctions among operational, intelligence, and hybrid activities determine applicable legal authorities, oversight requirements, and accountability regimes).

82. *See, e.g.*, Jennifer L. Selin & Pamela J. Clouser McCann, *Constraining the Executive Branch: Delegation, Agency Independence, and Congressional Design of Judicial Review*, 119 Nw. U. L. Rev. 1273, 1353-64 (2024) (explaining how the scope of discretion, congressional authorization, and the availability of judicial review determine the constitutional permissibility and constraint of executive-branch delegations).

83. *See* Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 Harv. J. L. & Tech. 117, 152-54 (2021) (explaining that algorithmic systems operate through and are shaped by overlapping institutional layers and bureaucratic logics, rather than through a single unified decisionmaker).

84. *See generally id.* at 153-55.

85. *See generally* Jake Kauffman, *Booz Allen and Palantir Partner to Boost U.S. Defense,* Defense and Munitions (Dec. 21, 2024), https://www.defenseandmunitions.com/news/booz-allen-and-palantir-partner-to-boost-us-defense/ [https://perma.cc/563D-YAHT].

At the oversight level, the Office of Legal Counsel (OLC), the National Security Council (NSC), and the White House AI Office may provide internal guidance on the legality and ethical dimensions of AI deployment.[86] Nevertheless, few of these bodies have transparent protocols for reviewing algorithmic models with foreign policy implications.[87] The diffusion of decision-making authority across classified settings, proprietary algorithms, and interagency silos inhibits the traditional checks embedded in the separation of powers.[88]

Notably absent from this multilayered architecture are robust roles for Congress and the judiciary. Congressional oversight of algorithmic foreign policy remains underdeveloped, partly due to the technical complexity of the systems and the institutional reluctance to confront executive prerogatives in national security.[89] Courts, meanwhile, are structurally constrained by doctrines of standing, the political question doctrine, and state secrets, all of which erect formidable barriers to reviewing AI-driven executive conduct abroad.[90]

Conceptualizing algorithmic foreign policy requires more than identifying technological innovation in statecraft; it demands a reconceptualization of how power is exercised, obscured, and institutionalized through code.[91] As AI systems increasingly mediate the formation and content of foreign relations, the constitutional and statutory frameworks governing executive agreements must evolve to preserve principles of transparency, legality, and democratic control.[92] Without such recalibration, algorithmic foreign policy might become a jurisprudential blind spot — highly consequential yet structurally elusive.

---

86. *See generally* Oona A. Hathaway, *National Security Lawyering in the Post-War Era: Can Law Constrain Power?*, 68 UCLA L. Rev. 2, 28–34 (2021) (describing the central role of OLC, NSC legal advisors, and White House legal offices in providing internal national-security legal oversight and constraining executive action).

87. *See generally* U.S. Gov't Accountability Off., GAO-21-519SP, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities 20–23 (2021) (identifying weaknesses in federal AI oversight structures and emphasizing the absence of standardized, transparent review protocols).

88. *See* Benedict Sheehy & Yee-Fui Ng, *The Challenges of AI Decision-Making in Government and Administrative Law: A Proposal for Regulatory Design*, 57 Ind. L. Rev. 665, 678–80 (2024) (explaining how AI-driven, opaque, and cross-agency decision processes hinder transparency and undermine the ability of legislative and judicial actors to exercise traditional oversight).

89. *See* Ünver *supra* note 71, at 1-10 (describing how algorithmic and automated diplomatic tools are developed within executive-branch structures, leaving Congress and the judiciary without comparable oversight capacity).

90. *See* Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 Colum. L. Rev. 1941, 1952, 1958-60 (2019) (explaining how standing, the political question doctrine, and the state secrets privilege limit judicial review of state action involving AI systems, particularly in security and foreign-affairs contexts).

91. H. Akın Ünver, *Computational International Relations: What Can Programming, Coding and Internet Research Do for the Discipline?*, 8 All Azimuth 157, 162–67 (2019) (arguing that computational tools reshape how political power is exercised and institutionalized by embedding decision rules and interpretive logics within code).

92. *See generally* Oona A. Hathaway, Curtis A. Bradley, & Jack L. Goldsmith, *The Failed Transparency Regime for Executive Agreements*, 134 Harv. L. Rev. 629, 642–55 (2020) (explaining that the existing statutory and reporting framework for executive agreements lacks sufficient transparency and congressional oversight, undermining legality and democratic control).

II. Constitutional Tensions and Doctrinal Gaps

The constitutional architecture of American foreign relations has long rested on doctrines and institutional arrangements designed for an era of human-directed statecraft. The rapid integration of AI into executive decision-making often exposes and exacerbates persistent doctrinal gaps and tensions.[93] As the boundaries between algorithmic operations and sovereign authority blur, longstanding principles governing accountability, judicial review, war powers, and delegation are strained to the breaking point.[94] This section critically examines the most pressing constitutional challenges raised by AI in foreign affairs, focusing on the erosion of oversight in executive agreements, the expansion of political question barriers through technological secrecy, the destabilization of war powers doctrine by algorithmic targeting, and the threat posed to the nondelegation principle by the disappearance of human judgment. Together, these tensions underscore the pressing need for doctrinal clarity and institutional adaptation in an era of automated governance.

A. Accountability in Executive Agreements

The constitutional design of U.S. foreign relations law presumes that executive action, even when undertaken without prior legislative approval, remains tethered to some form of legal or political accountability.[95] Executive agreements, particularly those executed without public disclosure, formal Senate oversight, or subsequent judicial review, pose structural risks to that principle.[96] The rise of algorithmically influenced foreign policy further complicates the calculus, creating new vectors for opacity and diminishing traditional channels of democratic control.[97] The foundational concern is that foreign commitments, once accountable to a tripartite system of governance, may increasingly operate in the shadows of code and unilateral discretion.[98]

---

93. *See generally* Ashley S. Deeks, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* viii–xiv (Oxford Univ. Press 2025) (explaining that constitutional and statutory frameworks premised on human-directed national-security decision-making are strained and destabilized by the opacity and autonomy of AI systems).

94. *See generally id.* at viii–xiv.

95. H. Jefferson Powell, *President's Authority over Foreign Affairs: An Executive Branch Perspective*, 67 Geo. Wash. L. Rev. 527, 546-55 (1999) (explaining that unilateral presidential actions in foreign affairs are constitutionally premised on mechanisms of legal, political, and institutional accountability).

96. *See id.* at 560-61.

97. *See, e.g.*, Robyn Caplan & Danah Boyd, *Mediation, Automation, Power*, *in* Who Controls the Public Sphere in an Era of Algorithms? 1, 4-11 (Data & Soc'y 2016) (explaining how algorithmic mediation introduces opacity, hidden prioritization, and diminished democratic control in decision environments).

98. *See generally* Tayo Fashoyin, *Tripartite Cooperation, Social Dialogue and National Development*, 143 Int'l Lab. Rev. 341, 345–48 (2004) (explaining how tripartite governance ensures accountability and how the weakening of one component leads to opaque, unilateral decision-making).

Article II of the Constitution grants the President the power to make treaties "by and with the Advice and Consent of the Senate."[99] However, in practice, executive agreements have largely supplanted treaties as the dominant mode of international commitment. A study by the Congressional Research Service found that "[f]rom 1980 to 1991, the United States entered 259 executive agreements, of which only 79 were treaties."[100] This shift is has not been found unconstitutional, as the Supreme Court has upheld congressional-executive and sole executive agreements in various contexts.[101] However, it has contributed to the erosion of the Senate's institutional role in shaping and reviewing foreign commitments.[102]

The absence of legislative participation means that many executive agreements are not subjected to rigorous public debate, statutory authorization, or post-ratification review.[103] The State Department's Circular 175 Procedure[104] provides internal guidelines for coordinating such agreements, but these are not binding on the President and are often applied inconsistently.[105] Even when agreements are reported to Congress under the Case-Zablocki Act,[106] delays and omissions are common, and classified or sensitive agreements may be withheld from public scrutiny entirely.[107]

This lack of transparency raises distinct constitutional questions in an era of algorithmic foreign policy. When AI-generated threat assessments, risk scores, or language models shape the content or logic of an executive

---

99. U.S. Const. art. II, § 2, cl. 2; *See also* Howard R. Sklamberg, *The Meaning of Advice and Consent: The Senate's Constitutional Role in Treatymaking*, 18 Mich. J. Int'l L. 445, 445-447 (1997) (tracing the historical and constitutional meaning of the Senate's "Advice and Consent" function in treaty formation, reemphasizing the reality that the President may make a treaty only if two-thirds of the Senate agrees to approve it after reviewing and considering the proposed international agreement).

100. Cong. Rsch. Serv., 66-922 CC, *Treaties and Other International Agreements: The Role of The United States Senate* 17 (2001), available at: https://www.gc.noaa.gov/documents/S.Prt_106-71_Treaties-Role_of_US_Senate_2001.pdf [https://perma.cc/32L8-FMND] (reporting that from 1980 to 1991 the United States concluded 259 executive agreements compared to only 79 treaties).

101. *See* Bradford R. Clark, *Domesticating Sole Executive Agreements*, 93 Va. L. Rev. 1573, 1574-76, 1607-17 (2007) (Clark's analysis directly supports the sentence's claim that the post-1980 shift toward executive agreements "has not been found unconstitutional," because Supreme Court doctrine has repeatedly validated these instruments.).

102. James M. Lindsay, *Congress, Foreign Policy, and the New Institutionalism*, 38 Int'l Stud. Q. 281, 283-287 (1994) (analyzing how the growing use of executive agreements has weakened Congress's, including the Senate's, role in foreign-policy oversight).

103. *See* Peter J. Spiro, *Treaties, Executive Agreements, and Constitutional Method*, 79 Tex. L. Rev. 961, 963-964 (2001) (noting that executive agreements circumvent the deliberative and accountability mechanisms associated with Senate-approved treaties).

104. U.S. Dep't of State, 11 FAM 720 (2006).

105. *See, e.g.,* Richard J. Erickson, *Status of Forces Agreements: A Sharing of Sovereign Prerogative*. 37 A.F. L. Rev. 137, 137-138 (1994) (observing that executive agreements, including SOFAs, rely on Circular 175 only as internal guidance and that its application varies across administrations).

106. Case-Zablocki Act, 1 U.S.C. § 112b (1972). The Act requires the executive branch to report all international agreements other than treaties to Congress within 60 days.

107. Curtis Bradley, *Amendments to the Case-Zablocki Act Concerning Reporting and Publication of International Agreements and Related Regulations (U.S.)*, 63 Int'l Legal Materials 275, 276-278 (2024) (describing persistent delays, incomplete reporting, and classification practices that limit access to international agreements despite Case-Zablocki requirements).

agreement, the opacity of the underlying model compounds the secrecy of the agreement itself.[108] Unlike conventional policymaking, where decisionmakers can be questioned and records subpoenaed, algorithmic influence is frequently shielded by proprietary code, national security classification, or technical inaccessibility.[109] In effect, foreign policy is not only removed from Senate advice and consent, but also from meaningful public intelligibility.

Perhaps the most constitutionally fraught feature of executive agreements is their practical insulation from judicial review. While courts have long acknowledged the validity of non-treaty foreign commitments, as in *Dames & Moore v. Regan*,[110] they have offered little doctrinal clarity on the legal enforceability or reviewability of such commitments, particularly where they are not codified in domestic law.[111] The result is a category of instruments that are legally binding on the international stage but often nonjusticiable in U.S. courts.[112]

This doctrinal lacuna becomes more consequential when algorithmic systems influence the terms or formation of an executive agreement. If, for instance, a machine-learning model incorrectly categorizes a foreign nation as an "advanced persistent threat,"[113] prompting the President to enter a bilateral agreement restricting technology exports, neither the algorithm's designation nor the executive's reliance on it would likely be subject to judicial scrutiny.[114] The convergence of the political question doctrine, state secrets privilege, and the non-reviewability of foreign policy decisions creates a legal vacuum in which consequential international actions, shaped by opaque and potentially flawed computational processes, escape both judicial and legislative accountability.[115]

---

108. *See generally* Deeks, *supra* note 93, at Viii-IX.

109. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–4, 102 (Harvard Univ. Press 2015) (explaining how proprietary rights, classification, and technical opacity render algorithmic systems resistant to oversight and disclosure).

110. Dames & Moore v. Regan, 453 U.S. 654 (659–61, 674–88 (1981) (The case upholds the President's authority to suspend claims and transfer attachments pursuant to emergency economic powers and longstanding congressional acquiescence, and articulating a functional framework for assessing executive power in foreign affairs in the absence of explicit statutory authorization.).

111. *See* Miller, *supra* note 33, at 1105-1107.

112. *See e.g.*, Machiko Kanetake & André Nollkaemper, *The Application of Informal International Instruments Before Domestic Courts*, 46 Geo. Wash. Int'l L. Rev. 765 (2014) (analyzing courts' reluctance to review or enforce informal international commitments that lack domestic codification).

113. Adel Alshamrani, et al., *A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities*, 21 IEEE Commc'ns Survs. & Tutorials 1851, 1853–56, 1865–68 (2019) (describing the characteristics and detection challenges of advanced persistent threats, including the potential for machine-learning systems to misclassify threat actors).

114. *See generally* Justin Shields, *Smart Machines and Smarter Policy: Foreign Investment Regulation, National Security, and Technology Transfer in the Age of Artificial Intelligence*, 51 J. Marshall L. Rev. 279, 286–92 (2018) (describing how AI-generated national-security risk assessments influence executive action while remaining largely insulated from judicial review).

115. *See*, e.g., Bancoult v. McNamara, 445 F.3d 427, 436 (D.C. Cir. 2006) (holding that establishment of a U.S. military base abroad "was an exercise of the foreign policy and

Moreover, where algorithmic outputs serve as informal predicates for diplomatic understandings, such as shared intelligence frameworks, interoperability protocols, or cyber-coordination pledges, there may be no formal agreement to scrutinize at all.[116] However, the material effects of these arrangements may mirror those of binding instruments, raising concerns about the circumvention of both the constitutional treaty process and statutory foreign policy constraints.[117]

Executive agreements have long existed in constitutional tension with the principles of transparency and democratic accountability.[118] The integration of AI into the foreign policymaking process intensifies these tensions, allowing commitments to be crafted, influenced, or justified through channels that are neither transparent to the public nor subject to judicial review.[119] Insofar as these algorithmically shaped agreements increasingly drive U.S. engagement abroad, they risk transforming the President's foreign affairs powers from a politically accountable prerogative into a technologically mediated domain largely immune from constitutional constraint. Without reform, whether through statutory reporting mandates, judicial engagement, or algorithmic disclosure requirements, this model of foreign policymaking threatens to subvert the constitutional architecture it purports to serve.

B. The Political Question Doctrine and AI-Driven Secrecy

Federal courts have long demonstrated restraint in adjudicating disputes that implicate the executive branch's conduct of foreign affairs, often invoking the political question doctrine as a threshold barrier to jurisdiction. Originally articulated in *Baker v. Carr*,[120] the doctrine has served as a doctrinal shield to preserve the separation of powers and to avoid judicial intrusion into diplomatically or militarily sensitive matters.[121] Recently, the National AI Initiative Act[122] attempted to establish a national AI policy, encourage federal agency coordination, and recognize the importance of AI for national security and

national security powers . . . and we could not reexamine the choice without making a 'policy determination of a kind clearly for nonjudicial discretion'").

116. United States v. Reynolds, 345 U.S. 1 (1953) (establishing the state secrets privilege permitting dismissal of cases where disclosure of evidence would "harm national-security interests").

117. Oona A. Hathaway, *Treaties' End: The Past, Present, and Future of International Lawmaking in the United States*, 117 Yale L.J. 1236, 1283–85 (2008) (documenting the increasing use of executive agreements and noting that their opacity undermines democratic accountability and congressional oversight).

118. *See* Curtis A. Bradley, International Law in the U.S. Legal System 67–72 (Oxford University Press, 2nd ed. 2015), (describing how executive agreements bypass the Senate advice-and-consent process and raise concerns regarding transparency, democratic oversight, and accountability).

119. *Id.* at 67-72.

120. Baker v. Carr, 369 US 186 (1962).

121. *See* Phil C. Neal, *Baker v. Carr: Politics in Search of Law*, 1962 Sup. Ct. Rev. 252, 256–60 (1962) (explaining how Baker articulated the modern political question doctrine and grounded judicial restraint in separation-of-powers principles).

122. *National Artificial Intelligence Initiative*, 15 U.S.C. §§ 9411-9415 (2024).

foreign policy.[123] However, the emergence of AI-driven foreign policy decision-making reveals an evolving dynamic: one in which the political question doctrine not only defers to executive discretion but also increasingly intersects with technological opacity, thereby shielding algorithmic decisions from constitutional scrutiny.[124]

The classic formulation of the political question doctrine is found in *Baker v. Carr*, where the Supreme Court identified six independent factors for determining whether a case presents a nonjusticiable political question, including a textually demonstrable constitutional commitment of the issue to a coordinate branch of government and a lack of judicially discoverable and manageable standards.[125] In the realm of foreign relations, the Court has often treated these factors as dispositive, particularly in matters of military engagement, treaty formation, or the recognition of foreign governments.[126]

For example, in *Goldwater v. Carter*,[127] the Court dismissed a challenge to President Carter's unilateral termination of a mutual defense treaty with Taiwan, with Justice Rehnquist writing that the matter involved the constitutional authority between the political branches not fit for judicial resolution.[128] Similarly, in *Harisiades v. Shaughnessy*,[129] the Court emphasized that any policy toward non-U.S. citizens are interwoven with contemporaneous policies regarding the conduct of foreign relations, further emphasizing its reluctance to review executive decisions in foreign policy domains.[130] This judicial reluctance has also extended to executive agreements. In *Dames & Moore v. Regan*,[131] the Court upheld a series of executive actions, including an agreement to terminate legal claims by U.S. nationals against Iran, on the basis of longstanding practice and implicit congressional acquiescence, even while acknowledging

123. Matthew R. Gaske, Regulation Priorities for Artificial Intelligence Foundation Models, 26 Vand. J. Ent. & Tech. L. 1 (2023) (discussing how federal initiatives, including the National AI Initiative Act, seek to coordinate U.S. AI policy and emphasize AI's national-security implications).

124. *See, e.g.,* Curtis A. Bradley & Trevor W. Morrison, *Presidential Power, Historical Practice, and Legal Constraint,* 113 Colum. L. Rev. 1095, 1120–27 (2013) (explaining that courts traditionally avoid reviewing foreign-affairs decisions and often treat them as nonjusticiable, reinforcing broad executive discretion).

125. *See, e.g.,* Guy-Uriel E. Charles, *Constitutional Pluralism and Democratic Politics: Reflections on the Interpretive Approach of Baker v. Carr*, 80 N.C. L. Rev. 1103, 1108–12 (2002) (describing the six factors identified in Baker v. Carr for determining whether a case presents a nonjusticiable political question).

126. Abner J. Mikva, Justice Brennan and the Political Process: Assessing the Legacy of Baker v. Carr, 1995 U. Ill. L. Rev. 683, 695–701 (explaining the structure and rationale of the Baker factors that courts later apply to foreign-relations controversies).

127. Goldwater v. Carter, 444 U.S. 996, 997 (1979) (Rehnquist, J., concurring).

128. Vincent John Paluzzi, Constitutional Law—Justiciability—Treaty Termination: A Nonjusticiable Controversy—Goldwater v. Carter, 100 S. Ct. 533 (1979), 11 Seton Hall L. Rev. 243, 244–49 (1980) (analyzing the Court's conclusion that treaty termination raised a political-branch dispute not suitable for judicial resolution).

129. Harisiades v. Shaughnessy, 342 U.S. 580, 588–89 (1952).

130. *See, e.g.*, James J. White, Constitutional Law: Search and Seizure: Search Incidental to an Administrative Arrest, 59 Mich. L. Rev. 306, 310–12 (1960) (noting the Court's view in Harisiades that regulation of non-U.S. citizens are intertwined with foreign-relations concerns and therefore warrants substantial judicial deference).

131. Dames & Moore v. Regan, 453 U.S. 654, 682–83 (1981).

the absence of explicit statutory authorization.[132] These cases collectively illustrate a posture of extreme judicial deference, grounded not only in respect for coordinate branches of government, but in the perceived impracticality of developing legal standards for diplomatic judgment.

AI compounds the doctrine's already deferential posture by introducing a deeper layer of inaccessibility.[133] Many AI systems deployed in national security contexts, such as predictive threat assessment platforms, natural language generation tools, or surveillance targeting algorithms, operate on nontransparent or classified logic.[134] Courts already struggle to engage with technical expert evidence, and the addition of proprietary or black-box AI architecture often renders algorithmic decisions unintelligible, even to the officials who rely on them.[135]

Where decision-making processes are not only politically sensitive but also technically inscrutable, courts may conclude that there is a "lack of judicially discoverable and manageable standards," reinforcing the second factor in *Baker v. Carr* and further insulating such decisions from review.[136] For instance, a court evaluating the legality of an executive agreement based on an AI-generated risk model may face insurmountable hurdles if the system's logic is classified, unexplainable, or developed by third-party defense contractors.[137]

This challenge mirrors concerns articulated in *United States v. Reynolds*,[138] where the Court upheld the government's invocation of the state secrets privilege, denying plaintiffs access to information deemed critical to national security.[139] AI-driven foreign policy decisions operate similarly—the rationale is often coded, classified, or both. The convergence of technological complexity and state secrecy effectively forecloses judicial review, not because the legal

---

132. *See* Miller, *supra* note 33; *See also* Sharon D. Liko, *The Settlement Claims Case: Dames & (and) Moore v. Regan*, 10 Denv. J. Int'l L. & Pol'y 577, 579–86 (1981) (analyzing the Court's reliance on historical executive settlement practice and congressional acquiescence to uphold claim-termination measures despite limited statutory authorization).

133. *See, e.g.*, Hin-Yan Liu, *The Power Structure of Artificial Intelligence*, 10 Law, Innov. & Tech. 197, 205–12 (2018) (examining how AI systems generate opacity and informational asymmetries that impede oversight and external scrutiny).

134. Oben Yapar, *Explainable AI in National Security: Enhancing Trust and Accountability* 10 Int'l J. of Emerging Techs. and Innovative Res. h691, h694–h700 (2023) (describing how national-security AI systems frequently rely on opaque or classified model architectures that limit transparency and explainability).

135. *See* Edward Koellner, Black Box Justice? Legal Evidence, Digital Democracy, and the Risks of AI in Hyper-Specialized Courts, conf. paper at 4–8, 25th Int'l Roundtable for the Semiotics of Law (2025) (explaining that courts struggle to evaluate complex or opaque AI-generated evidence, particularly when the systems operate as black boxes inaccessible even to government officials).

136. Baker v. Carr, 369 U.S. 186, 217 (1962) (identifying the absence of "judicially discoverable and manageable standards" as a core basis for deeming an issue nonjusticiable under the political-question doctrine).

137. Amy J. Schmitz, *Responsible Use of AI in Civil Dispute Resolution*, *in* The Cambridge Handbook on AI and Civil Dispute Resolution (forthcoming 2025 or 2026) (manuscript at 12–17) (discussing how proprietary, unexplainable, or confidential AI systems impede judicial scrutiny and limit courts' ability to evaluate algorithmic reasoning).

138. United States v. Reynolds, 345 U.S. 1, 10 (1953).

139. Louis Fisher, The State Secrets Privilege: Relying on Reynolds, 122 Pol. Sci. Q. 385, 386–94 (2007) (examining the Court's deference to executive claims of national-security secrecy in United States v. Reynolds).

question is inherently unanswerable, but because the process of answering it has been architected to resist scrutiny.[140]

The political question doctrine rests on the premise that politically accountable actors make decisions.[141] Nevertheless, algorithmic decision-making introduces ambiguity into that assumption. When AI systems effectively generate, prioritize, or filter foreign policy options, especially without meaningful human oversight, they blur the line between delegated support and delegated authority.[142] Algorithmic delegation in executive decision-making may lead to a diffusion of responsibility, challenging the democratic structure of constitutional accountability.[143] In such cases, the doctrine may be invoked not simply to protect political discretion, but to shield decisions made by non-human agents. It risks transforming the political question doctrine into a judicial endorsement of governance by proxy, where algorithmic tools, not constitutionally designated officials, are the true authors of U.S. foreign policy.[144] Courts, by reflexively invoking the political question doctrine, may thus entrench a model of executive power that is unreviewable not only because it is politically sensitive, but because it is technically inscrutable.[145]

The political question doctrine was intended as a safeguard against judicial overreach in politically delicate areas of governance.[146] However, in the context of algorithmic foreign policy, it may serve instead as a doctrinal conduit through which executive discretion merges with technological opacity, thereby evading constitutional accountability.[147] As AI systems increasingly shape both

140. Tatiana Dancy & Monika Zalnieriute, *AI and Transparency in Judicial Decision-Making*, Oxford J. Legal Stud. (2025) (observing that "judicial reliance upon predictive AI tools is not always compatible with [transparency]" and that in cases involving "trade secrecy and/or machine learning," transparency, which underpins judicial review, is largely unattainable).

141. *See, e.g.*, Jesse H. Choper, *The Political Question Doctrine: Suggested Criteria*, 54 Duke L.J. 1457, 1461–66 (2004) (explaining that the political question doctrine is premised on the notion that decisions in certain constitutional domains should be made by politically accountable branches rather than the judiciary).

142. *See generally* Martin Ebers & Henrik Trasberg, *Delegation of Administrative Powers to AI Systems*, *in* Artificial Intelligence and Machine Learning Powered Public Service Delivery in Estonia: Opportunities and Legal Challenges 85-102 (Cham: Springer International Publishing, 2023) (explaining how AI systems that generate or filter options can shift from decision support to de facto decision-making authority, particularly when human oversight is limited).

143. Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 Admin. L. Rev. 1, 20–28 (2019)(explaining how algorithmic opacity and distributed decision processes obscure lines of responsibility in government decision-making, thereby undermining traditional mechanisms of democratic accountability).

144. Andrew Chin, *The Black Box Presidency*, Univ. N.C. Sch. L. Legal Stud. Res. Paper Series, No. 5158692, at 5–6 (Feb. 27, 2025) (arguing that algorithmically driven decision-making in the executive branch may escape constitutional checks, turning courts into passive endorsers of "governance by proxy").

145. Richard Mackenzie-Gray Scott & Lilian Edwards, *The Inscrutable Code? The Deficient Scrutiny Problem of Automated Government*, 2025 Tech. & Regul. 37, 40–47 (2024) (arguing that automated government systems create opacity that impedes judicial scrutiny and may render executive action effectively unreviewable).

146. *See* Curtis A. Bradley & Eric A. Posner, *The Real Political Question Doctrine*, 75 Stan. L. Rev. 1031, 1033–34 (2023) (explaining that lower courts frequently invoke the political question doctrine in foreign-policy contexts to defer to executive discretion).

147. *See* David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 Yale J. Regul. 800, 812–24 (2020) (explaining how opaque

the content and conduct of foreign relations, courts must grapple with the reality that the grounds for nonjusticiability are being reconstructed less by law than by code.[148] A jurisprudence that fails to adapt to this transformation risks not only irrelevance, but complicity in the displacement of constitutional actors by computational processes.[149]

C. War Powers, Hostilities, and Algorithmic Targeting

The War Powers Resolution (WPR) was designed to restore congressional oversight in decisions to introduce U.S. forces into "hostilities," but its constitutional logic presumes human agency and observable conflict.[150] As the deployment of AI in military targeting expands, these foundational assumptions become obsolete.[151] The doctrinal gaps exposed by algorithmic decision-making are particularly acute when considering what constitutes "hostilities" under the WPR—and whether the law can meaningfully regulate military actions when the decision to use force is made not by a commander-in-chief, but by an autonomous system.[152]

Historically, both executive practice and judicial commentary have treated "hostilities" as a factual question, typically linked to sustained armed conflict or the risk thereof, and presupposing human deliberation.[153] The rise of AI-enabled targeting defies the clear assignment of responsibility that is central to both domestic and international law. In kinetic contexts, such as drone operations, when an AI selects and engages a target without direct human intervention, the trigger for WPR notification becomes uncertain.[154] The situation

---

algorithmic systems can expand discretionary government power and undermine judicial and institutional accountability).

148. Paul Evans, *Conclusion: So, What Is Good Scrutiny Good For?* 72, Parliamentary Aff. 987, 987–90 (2019) (arguing that modern governance increasingly limits scrutiny through opaque procedural and technological systems rather than through formal legal constraints).

149. Aziz Z. Huq, *A Right to a Human Decision*, 106 Va. L. Rev. 611, 611, 670–71 (2020) (highlighting that "[recent advances] have spurred anxiety about a shift of power from human to machine decision makers," and warning that failure to preserve a "right to a human decision" may leave constitutional roles hollow and displaced).

150. Mariah Zeisberg, *War Powers: The Politics of Constitutional Authority* 115–17 (Princeton University Press, 2013) (discussing how the War Powers Resolution reasserts congressional authority over hostilities that are human-directed and observable, and how its framework assumes such direct agency in armed conflict); *see also* Matthew C. Weed, Cong. Rsch. Serv., The War Powers Resolution: Concepts and Practice 2-3 (2015).

151. Scott Sullivan & Iben Ricket, *Targeting in the Black Box* 145–52 (16th Int'l Conf. on Cyber Conflict, 2024), https://ccdcoe.org/uploads/2024/05/CyCon_2024_Sullivan_Ricket-1.pdf [https://perma.cc/MZE8-C4XU] (explaining how autonomous targeting systems undermine traditional assumptions of human judgment, control, and accountability in the use of force).

152. Jimena Sofía Viveros Álvarez, *The Risks and Inefficacies of AI Systems in Military Targeting Support*, Humanitarian L. & Pol'y 4–10 (2024) (explaining how autonomous targeting systems undermine legal frameworks governing the use of force by introducing opacity, unpredictability, and diminished human control).

153. *See* Erica H. Ma, *The War Powers Resolution and the Concept of Hostilities*, 13 Ne. U.L. Rev. 519, 526–34 (2021) (reviewing executive and judicial interpretations of "hostilities" as a fact-specific inquiry grounded in human assessment of armed conflict).

154. *See* Anastasia Roberts & Adrian Venables, The Role of Artificial Intelligence in Kinetic Targeting from the Perspective of International Humanitarian Law, conf. paper at 5–11, 13th Int'l Conf. on Cyber Conflict (2021) (discussing how autonomous targeting

is even more complex in cyberwarfare, where AI-driven operations may disrupt critical infrastructure or sow chaos abroad without resorting to physical violence or direct attribution, raising the question of whether such activities amount to "hostilities" at all.[155]

As algorithmic targeting diffuses the locus of decision-making, it also challenges the capacity for congressional and judicial oversight. Responsibility for erroneous or escalatory actions, which are traditionally vested in the President or identifiable military officers, becomes opaque when AI systems operate with a high degree of autonomy.[156] The erosion of meaningful control and accountability mechanisms threatens the constitutional structure that the WPR was designed to protect. The challenge is not limited to the practical impossibility of oversight in classified or technologically complex settings; rather, it is the transformation of the concept of hostility itself, as warfare increasingly comprises actions that can produce real and devastating effects through code and algorithms.[157]

In this context, doctrinal stagnation risks leaving consequential decisions beyond the reach of constitutional checks.[158] If Congress cannot clearly determine when hostilities begin, or who is accountable for their initiation, the WPR's capacity to constrain the executive is fundamentally undermined.[159] In the age of algorithmic targeting, only a recalibration of war powers doctrine that recognizes both the realities of AI-driven conflict and the imperatives of democratic accountability can restore the constitutional balance.[160]

D. The Nondelegation Doctrine and the Disappearance of Human Judgment

The emergence of AI as a tool of foreign policy and national security has revived longstanding constitutional debates about the limits of executive power and the permissible scope of delegation under Article I.[161] At the core

systems obscure responsibility for kinetic actions and complicate legal triggers for the use of force).

155. Allison Arnold, *Cyber "Hostilities" and the War Powers Resolution*, 217 Mil. L. Rev. 174, 182–92 (2013) (explaining that non-kinetic cyber operations lacking physical violence or clear attribution challenge traditional understandings of "hostilities" under the WPR).

156. Dustin A. Lewis, Gabriella Blum & Naz K. Modirzadeh, *War-Algorithm Accountability*, Rsch. Briefing, Harv. L. Sch. Program on Int'l L. & Armed Conflict 6–15 (2016) (analyzing how autonomous targeting systems obscure the locus of decision-making and complicate legal and institutional mechanisms for assigning responsibility).

157. *Id.* at 6-15.

158. Yaniv Roznai & Tamar Hostovsky Brandes, *Democratic Erosion, Populist Constitutionalism, and the Unconstitutional Constitutional Amendments Doctrine*, 14 L. & Ethics of Hum. Rights, 19, 24–31 (2020) (arguing that constitutional doctrines must evolve when underlying political or structural realities change, lest significant exercises of state power fall outside effective constitutional scrutiny).

159. Matthew C. Waxman, *The Power to Threaten War*, 123 Yale L.J. 1626, 1646–52 (2014) (explaining that ambiguity about when hostilities begin and who initiates them erodes Congress's ability to exercise effective war-powers oversight).

160. See, e.g., Dumitru Budacu, *The Impact of the Artificial Intelligence on Hybrid Conflicts in the 21st Century*, 18 Studia Securitatis 87, 92–99 (2024) (explaining how AI-driven conflict alters traditional mechanisms of control and accountability, necessitating legal and doctrinal adaptation).

161. Thomas W. Merrill, *Rethinking Article I, Section I: From Nondelegation to Exclusive Delegation*, 104 Colum. L. Rev. 2097, 2106–17 (2004) (discussing how evolving forms

of the nondelegation doctrine lies the principle that Congress may not cede legislative authority to another branch without providing an "intelligible principle" to guide discretion.[162] However, as the executive increasingly relies on algorithmic systems to inform or even make foreign policy decisions, the doctrinal foundations of nondelegation are tested in ways that traditional jurisprudence did not foresee.[163]

Historically, courts have adopted a functionalist approach to delegation in the national security context, granting the executive branch substantial leeway based on both necessity and expertise.[164] The Supreme Court's refusal to enforce rigid separation-of-powers boundaries during moments of perceived emergency has effectively insulated vast swaths of foreign relations and security policy from meaningful legislative constraint.[165] Functionalism, justified by the unpredictability of foreign threats and the need for rapid executive action, is now confronted by a new dilemma: the replacement of human judgment with automated, opaque, and potentially unaccountable algorithmic processes.[166]

The rise of AI-driven policy mechanisms raises the question of whether delegation to non-human agents, which are systems that lack reason, accountability, or interpretive capacity, can ever satisfy the constitutional demands of the nondelegation doctrine. Algorithmic decision-making supplants traditional forms of public and congressional oversight, potentially undermining the core logic of constitutional accountability.[167] In areas where algorithms operate with high autonomy, functionalist justifications risk collapsing into abdication, as even minimal "intelligible principles" may fail to constrain the behavior of complex and evolving AI systems.[168] In national security, the opacity

---

of policymaking revive constitutional debates about executive power and the limits of delegation under Article I).

162. Gary Lawson, *Discretion as Delegation: The Proper Understanding of the Nondelegation Doctrine*, 73 Geo. Wash. L. Rev. 235, 239–48 (2005) (explaining that Congress violates the nondelegation doctrine when it transfers discretionary authority without supplying an "intelligible principle" to guide its exercise).

163. *See generally* Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. Pa. L. Rev. 1347, 1373–77 (2016) (explaining how autonomous systems displace human decision-making and create responsibility gaps, thereby challenging traditional legal frameworks grounded in human discretion).

164. Robert Knowles, *Delegating National Security*, 98 Wash. U. L. Rev. 1117, 1124–38 (2021) (explaining that courts traditionally adopt a functionalist, deferential approach to delegation in national security because of executive expertise, secrecy needs, and institutional limitations).

165. Curtis A. Bradley and Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2047, 2096–2101 (2005) (describing how judicial deference in national-security emergencies weakens separation-of-powers enforcement and allows expansive executive action absent clear congressional constraint).

166. Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1784–1800 (2019) (explaining how machine-learning technologies introduce opacity and undermine human judgment in national-security decision-making).

167. Crootof, *supra* note 163, at 1357.

168. Amit Haim, *The Administrative State and Artificial Intelligence: Toward an Internal Law of Administrative Algorithms*, 14 U.C. Irvine L. Rev. 103, 118–29 (2024) (arguing that traditional delegation doctrines provide insufficient constraints on autonomous algorithmic systems whose complexity and evolution undermine meaningful oversight).

of algorithmic decision-making could render traditional checks ineffective, eroding the values that undergird the separation of powers.[169]

If the essence of lawmaking is the exercise of judgment, then delegating core policy decisions to machines, entities incapable of political or moral reasoning, arguably contravenes the very premise of the nondelegation doctrine.[170] Formalist perspectives further underscore the threat posed by algorithmic outsourcing, warning that the disappearance of human judgment in areas as consequential as foreign policy may not merely challenge existing doctrine but also undermine foundational principles of democratic governance and constitutional structure.[171]

Ultimately, the constitutional legitimacy of AI-driven foreign policy may depend on whether the executive can meaningfully supervise and be held accountable for the actions of its algorithmic agents.[172] Without robust oversight and clear limits, the deployment of AI risks transforming the executive's delegated discretion into a black box, irreconcilable with both functionalist and formalist interpretations of the nondelegation doctrine.[173] The challenge for courts and Congress will be to articulate new frameworks that ensure the enduring centrality of human judgment in the making and execution of national security policy.[174]

III. A Framework for Algorithmic Legal Accountability

The profound challenges posed by AI in foreign relations demand more than mere adaptation of existing doctrines; they require a principled framework capable of anchoring algorithmic decision-making within the bounds of constitutional accountability and transparency.[175] As legal scholarship has

169. David Freeman Engstrom, *The Automated State: A Realist View*, 92 Geo. Wash. L. Rev. 1437, 1458–66 (2024) (explaining how algorithmic opacity in government decision-making impedes judicial and legislative oversight, thereby straining separation-of-powers constraints).

170. Keith E. Whittington & Jason Iuliano, *The Myth of the Nondelegation Doctrine*, 165 U. Pa. L. Rev. 379, 390–403 (2016) (explaining that the nondelegation doctrine rests on the premise that discretionary policymaking requires human judgment and political accountability).

171. Rónán Kennedy & W. Barfield, The Rule of Law and Algorithmic Governance, *in* Cambridge Handbook of the Law of Algorithms 209, 214–22 (Cambridge University Press 2020) (explaining that algorithmic systems can displace human judgment and undermine core rule-of-law and constitutional accountability principles).

172. *See, e.g.*, Eva Erman & Markus Furendal, *Artificial Intelligence and the Political Legitimacy of Global Governance*, 72 Pol. Stud. 421, 425–33 (2022) (arguing that the legitimacy of AI-mediated governance depends on maintaining meaningful human oversight and accountability for algorithmic actions).

173. Matthew R. Gaske, *The Operational Paradox of Centralized Artificial Intelligence Regulation*, 2024 Mich. St. L. Rev. 367, 380–92 (2024 (explaining how opaque AI systems can undermine both functionalist and formalist limits on delegated governmental authority).

174. *See generally* Derigan Silver, *Power, National Security and Transparency: Judicial Decision Making and Social Architecture in the Federal Courts*, 15 Commc'n L. & Pol'y 129, 140–49 (2010) (examining how judicial oversight in national-security cases depends on transparent, human-driven decision structures and accountability norms).

175. Gilad Abiri, *Public Constitutional AI*, 59 Ga. L. Rev. 601, 603–10 (2025) (arguing that governments must adopt a principled constitutional framework to ensure accountability

recognized, the exceptionalism long afforded to foreign affairs cannot justify a retreat from core democratic safeguards in the age of autonomous systems.[176] This section outlines a structured approach to algorithmic legal accountability, starting with its normative foundations, proposing a concrete set of statutory and institutional reforms, and drawing on comparative insights from international regulatory efforts. By clarifying the legal and procedural boundaries for AI in statecraft, the framework aims to ensure that technological innovation proceeds in step with enduring commitments to transparency, human judgment, and the rule of law.

A. Normative Foundations

The rapid integration of AI into U.S. foreign policy and national security decision-making demands a robust normative framework to ensure legal accountability.[177] While the imperatives of national security and diplomatic agility have often justified broad executive discretion, the unique risks posed by algorithmic systems render continued exemption of foreign relations from meaningful oversight untenable.[178]

At stake is the core principle that no governmental domain, regardless of technological sophistication or geopolitical urgency, can operate beyond the reach of legal accountability.[179] The opacity, speed, and unpredictability of AI-driven decision-making amplify the dangers historically associated with unchecked executive authority, particularly when consequential choices, such as treaty commitments or the use of force, are made without clear lines of human deliberation or public transparency.[180] Without enforceable legal constraints, algorithmic governance risks undermining democratic legitimacy and eroding foundational checks on state power.[181]

A commitment to transparency, with meaningful human oversight through human-in-the-loop approaches and interpretability, must form the backbone of

---

and transparency in public-sector AI systems, rather than relying on incremental doctrinal adaptation).

176. K. J. Holsti, *Exceptionalism in American Foreign Policy: Is it Exceptional?*, 17 Euro. J. Int'l Rel. 381, 386–92 (2011) (analyzing the roots and limits of foreign-policy exceptionalism and questioning its compatibility with democratic accountability).

177. Crootof, *supra* note 163, at 1357.

178. Jelena Vujicic, *Algorithmic Accountability and Ethical Oversight: Legal Challenges in Transatlantic AI Regulation*, 13 Int'l J. of Rsch. and Sci. 4409, 4412–17 (2024) (explaining how algorithmic opacity and risk in security and governance contexts make traditional exemptions from oversight increasingly untenable).

179. John Ramming Chappell, *Towards Accountability: US Investigations of Civilian Harm under International Law*, 29 UC Davis J. Int'l L. & Pol'y 1, 10–22 (2022) (arguing that even technologically complex and security-sensitive military actions remain subject to legal accountability obligations).

180. *See generally* Fariha Ambreen Chaudhry, *AI-Powered Decision-Making: Balancing Automation and Human Oversight in Corporate Governance*, 1.1 Int'l J. Bus. & Comp. Sci. 10, 14–18 (2024) (explaining how opaque and rapid AI systems undermine accountability and human oversight, a dynamic that similarly heightens risks when applied to high-stakes governmental decision-making).

181. Crootof, *supra* note 163.

any normative framework for AI in foreign relations.[182] Transparency is not merely an abstract ideal, but a practical necessity for both public accountability and effective congressional oversight.[183] Algorithmic opacity is antithetical to the constitutional principle of open government, particularly where public scrutiny and judicial review are essential safeguards against abuse.[184] Human-in-the-loop requirements further ensure that critical decisions remain anchored in discernible judgment and moral responsibility, preserving the constitutional role of deliberative reasoning even as technical systems evolve.[185] Interpretability, meanwhile, is indispensable for both ex ante and ex post review, allowing for a meaningful assessment of how and why algorithmic decisions were made.[186]

The rise of AI in foreign affairs thus presents not only doctrinal challenges but profound normative questions. It is incumbent on lawmakers, judges, and scholars to reaffirm that constitutional principles, including transparency, oversight, and the indispensability of human judgment, remain vital even, and especially, as the mechanics of statecraft become increasingly complex.[187] Foreign relations cannot be treated as a constitutional "black box" simply because its tools have changed; to do so would abdicate both legal and democratic responsibility.[188]

B. Proposed Framework

Crafting legal architecture capable of constraining AI-driven foreign relations requires moving beyond aspirational principles to a set of enforceable rules, institutional triggers, and procedural checks.[189] Building on the normative foundations articulated above, this section proposes an accountability framework that draws from constitutional structure and administrative law.

---

182. Fabio Massimo Zanzotto, *Human-in-the-loop Artificial Intelligence*, 64 J. A.I. Rsch. 243, 245–52 (2019) (explaining that human oversight and interpretability are essential components of responsible and transparent AI systems).

183. Francesca Bignami, *Artificial Intelligence Accountability of Public Administration*, 70 Am. J. of Compar. L. i312, i318–27 (2022) (arguing that transparency is essential to enabling public accountability and effective institutional oversight of AI-driven administrative systems).

184. Giancarlo Frosio, *Algorithmic Enforcement Tools: Governing Opacity with Due Process*, *in* Driving Forensic Innovation in the 21st Century: Crossing the Valley of Death 195, 198–207 (Simona Francese & Roberto S. P. King, eds., 2024) (explaining how algorithmic opacity undermines transparency, due process, and meaningful judicial review).

185. Eduardo Mosqueira-Rey et al., *Human-in-the-Loop Machine Learning: A State of the Art*, 54 A.I. Rev. 3005, 3010–20 (2023) (explaining that HITL frameworks maintain human responsibility, interpretability, and ethical judgment in high-stakes AI decisions).

186. Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, 38 AI Mag. 50, 53–54 (2017) (explaining that interpretability is essential to enable both preventive and retrospective evaluation of algorithmic decisions).

187. *See* Aziz *supra* note 149, at 613 (2020).

188. *See generally* Deeks, *supra* note 93, at viii–xiii.

189. Mireille Hildebrandt, *Algorithmic Regulation and the Rule of Law*, 376 Phil. Trans. Royal Soc'y A, 20170355, 3–7 (2018) (arguing that effective governance of algorithmic systems requires enforceable legal rules, institutional safeguards, and procedural mechanisms to maintain the rule of law).

Certain domains, most notably the initiation of treaties and armed conflict, demand categorical exclusion of fully autonomous AI decision-making.[190] No machine, regardless of sophistication, should wield the sovereign prerogative to bind the nation to international obligations or deploy military force.[191] Congressional enactment of explicit statutory bars on the use of autonomous AI for such threshold decisions would codify a bright-line limitation and reassert the constitutional requirement for human deliberation at the apex of state power.[192]

Judicial review mechanisms must adapt to the gradations of AI autonomy in executive action.[193] Functional "autonomy triggers", which are defined by the level of algorithmic discretion in a given process, can serve as legal thresholds for when courts are required to intervene.[194] For instance, where an AI system exercises substantial independent judgment in the execution of foreign policy, especially about military actions, statutory provisions should mandate expedited judicial review to test for constitutional compliance, due process, and statutory authorization.[195] This dynamic approach to justiciability helps to ensure that the judiciary remains an active check even as the nature of executive action evolves.

Robust procedural requirements are essential to counteract the opacity and velocity of algorithmic decision-making.[196] Mandating public reporting of algorithmic use in sensitive foreign relations, algorithmic impact assessments, and ex ante publication of system capabilities and limitations can help foster

---

190. *See* Rebecca Crootof, *Autonomous Weapon Systems and the Limits of Analogy*, 9 Harv. Nat'l Sec. J. 51, 78-80 (2018) (arguing that fully autonomous systems must be categorically excluded from certain high-stakes decisions, particularly those involving the initiation or escalation of armed conflict).

191. *See generally* Kristian Humble, *Artificial Intelligence, International Law and the Race for Killer Robots in Modern Warfare*, *in* Artificial Intelligence, Social Harms and Human Rights 57, 59–66 (eds., Springer Nature 2023) (explaining that autonomous systems cannot satisfy the human-agency and accountability requirements necessary for lawful decisions on treaty obligations or the use of force).

192. Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained*, 16 J. L. Tech. & Internet 223, 240–47 (2025) (describing how Congress uses explicit statutory limits and categorical safeguards to regulate AI in sensitive domains, supporting the argument for bright-line prohibitions in sovereign decision-making).

193. Igor Gontarz, *Judicial Review of Automated Administrative Decision-Making: The Role of Administrative Courts in the Evaluation of Unlawful Regimes*, ELTE L. J. 151, 158–66 (2023) (arguing that judicial review frameworks must adapt to differing levels of automation and transparency in algorithmic decision-making).

194. *See, e.g.*, Nathan Gabriel Wood, *Autonomous Weapon Systems and Responsibility Gaps: A Taxonomy*, 25 Ethics & Info. Tech. 15, 18–24 (2023) (developing a taxonomy of algorithmic autonomy levels and explaining how rising autonomy creates responsibility gaps that necessitate distinct regulatory and oversight triggers).

195. Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 Harv. Nat'l Sec. J. 379, 401–12 (2017) (explaining that increasing levels of autonomy in weapon systems reduce human control and create accountability gaps, necessitating strengthened legal and oversight mechanisms).

196. Stephan Grimmelikhuijsen &Albert Meijer, *Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response*, 5 Persp. on Pub. Mgmt. & Governance 232, 236–44 (2022) (identifying opacity and rapid automated decision-making as key legitimacy risks and arguing for procedural safeguards to counteract them).

transparency and public trust.[197] Such measures align with emerging standards in administrative law and directly address the concerns that informational asymmetry surrounding AI decision-making undermines oversight and accountability.[198] Algorithmic impact assessments, modeled after environmental or privacy impact statements, would create a documented record for both congressional and judicial review, providing a basis for substantive evaluation of executive discretion.[199]

Finally, existing statutes governing war powers and international economic emergency authorities require targeted amendment to encompass algorithmic delegation.[200] The War Powers Resolution and International Emergency Economic Powers Act should be revised to include explicit requirements for reporting, human certification, and congressional notification when AI systems are used to implement or recommend the exercise of such powers.[201] These amendments would restore the centrality of congressional oversight, ensuring that evolving technologies do not become a vehicle for bypassing democratic control.

Through categorical constraints, adaptive review, procedural rigor, and renewed legislative oversight, this framework aims to reconcile technological innovation with enduring constitutional values. Effective accountability in the age of algorithmic governance will require not merely new statutes but a revitalized commitment to the principles of human agency, transparency, and democratic control at the heart of the American legal order.[202]

C. Comparative and International Analogues

The challenge of ensuring legal accountability for AI-driven decision-making in foreign relations is not unique to the United States.[203] Comparative and international legal developments offer instructive examples and cautionary

197. Emanuel Moss, et al., Assembling Accountability: Algorithmic Impact Assessment for the Public Interest, Data & Soc'y 6–14 (2021) (explaining how algorithmic impact assessments and public disclosure obligations enhance transparency and institutional trust in high-risk governmental AI systems).

198. Sheehy & Ng, *supra* note 88.

199. Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 Harv. J. L. & Tech. 117, 131–46 (2021) (arguing that algorithmic impact assessments create a documented record enabling meaningful legislative and judicial oversight of opaque algorithmic systems).

200. Denise Garcia, *Algorithms and Decision-Making in Military Artificial Intelligence*, 38 Glob. Soc'y 24, 28–34 (2024) (arguing that existing war-powers and security statutes are ill-equipped to regulate AI-driven decision systems and therefore require targeted reform).

201. *See generally* Def. Innovation Bd., AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense: Supporting Document 10–18 (2019), *available at* https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/oct/cs2019_0292.pdf [https://perma.cc/P7JM-7KVD] (recommending human oversight, traceability, and documentation requirements for AI systems used in national-security decision-making).

202. *See generally* Ben Chester Cheong, *Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making*, 6 Frontiers Hum. Dynamics 1421273, 4–6 (2024) (emphasizing that effective AI governance depends on transparency, human oversight, and institutional accountability mechanisms).

203. *See generally* John Kurre, *The Accountability, Responsibility & Governance as a Unified Strategy for AI* Nat'l Am. Univ. (2024).

lessons, demonstrating both the promise and the limits of regulatory innovation in this evolving domain. Transnational approaches to AI governance reveal both convergence on baseline accountability principles and persistent divergence over the treatment of foreign affairs and national security.[204]

The European Union's AI Act (AIA) stands as the most ambitious legislative effort to date to regulate high-risk AI systems, setting robust standards for transparency, risk management, and human oversight.[205] However, the AIA contains explicit carve-outs for military, defense, and national security applications, excluding much of foreign policy from its central accountability mechanisms.[206] While the AIA's risk-based classification and mandatory human-in-the-loop requirements provide a valuable template for procedural safeguards, its foreign affairs exemptions highlight a persistent reluctance among democratic states to fully subject national security functions to algorithmic oversight regimes.[207] The domains where AI poses the gravest risks are often those least likely to be regulated under prevailing frameworks.

Nevertheless, certain AIA provisions offer models for adaptation. For example, requirements for algorithmic transparency, documentation, and impact assessment, while not presently applied to defense or foreign affairs, could be selectively incorporated into U.S. legal frameworks, especially where national security interests do not preclude public or legislative scrutiny.[208] The European experience demonstrates both the feasibility of sector-specific regulation and the political difficulty of achieving comprehensive oversight in matters of statecraft.

International Humanitarian Law (IHL), particularly as embodied in the Geneva Conventions and related protocols, has long confronted questions of accountability for autonomous weapons and decision-making systems.[209]

---

204. *See, e.g.*, Artur Ishkhanyan, *The Sovereignty-Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control*, 5.123 Discover A.I. 4–7 (2025) (discussing the simultaneous convergence of accountability standards and divergence in national-security and foreign-affairs approaches to AI governance).

205. Junaid Sattar Butt, *Analytical Study of The World's First EU Artificial Intelligence (AI) Act*, 5 Int'l J. Rsch. Publ'n & Revs. 7343 7348–50 (2024) (analyzing the AIA's requirements for high-risk AI systems, including transparency obligations, risk-management duties, and human-oversight safeguards).

206. Roger Clarke, *An Evaluation of the EU AI Act Against the Normative Framework for Regulatory Regimes* 12–15 (SSRN Working Paper, Paper No. 5244054, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5244054 [https://perma.cc/L8TC-U2PC] (discussing the AIA's exemptions for military, defense, and national-security uses and noting that these carve-outs remove such systems from the Act's accountability requirements).

207. Georgios Pavlidis, *Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI*, 16 L. Innovation & Tech. 293, 305–10 (2024) (explaining how the AIA's risk-based safeguards and human-oversight requirements structure accountability for high-risk systems, while noting that these mechanisms apply only within the Act's regulated scope).

208. Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 Commc'n. ACM 56, 56–60 (2016) (identifying transparency, documentation, and impact-assessment practices as core mechanisms for algorithmic accountability, thereby illustrating why such procedures could be adapted for legal oversight frameworks beyond the AIA).

209. Kjølv Egeland, *Lethal Autonomous Weapon Systems under International Humanitarian Law,* 85 Nordic J. Int'l L. 89 92–104 (2016) (analyzing how IHL doctrines grounded in the Geneva Conventions address accountability, responsibility, and compliance challenges posed by autonomous weapon systems).

Recent diplomatic and expert debates, such as those within the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems, have converged on the need to preserve "meaningful human control" over life-and-death decisions.[210] IHL thus offers a clear normative anchor: delegation to machines must never eliminate human responsibility, particularly where fundamental rights and the laws of armed conflict are implicated.[211] While the legal enforceability of such principles remains contested, the focus on individual and state accountability in IHL has shaped emerging domestic and international proposals for algorithmic governance.[212] The insistence on human control is not just a moral imperative, but a practical necessity for ensuring that legal systems can adapt to technological change.[213] It is expected that efforts to operationalize this standard through audit trails, command responsibility doctrines, and robust review procedures, may offer a path forward for regulating AI in both foreign relations and national security.

The divergence in regulatory approaches between the United States, the European Union, and international humanitarian law underscores the need for a transnational dialogue on algorithmic accountability.[214] Legal frameworks must address not only the risks of domestic circumvention but also the prospect of regulatory arbitrage and the erosion of fundamental legal norms.[215] Without foundational norms of openness, supervision, and meaningful human involvement, the rapid international adoption of AI in government decision-making risks advancing well beyond the reach of robust legal regulation. Comparative and international analogues thus underscore both the necessity and the difficulty of building a robust accountability regime for algorithmic

210. *See e.g.*, Michael W. Meier, *Lethal Autonomous Weapons Systems (Laws): Conducting a Comprehensive Weapons Review*, 30 Temp. Int'l & Comp. L. J. 119 128–32 (2016) (explaining that compliance with IHL necessitates retaining human judgment over lethal targeting decisions, a premise that parallels the GGE's emphasis on "meaningful human control").

211. *See generally* Markus Wagner, *The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems*, 47 Vand. J. Transnat'l L. 1371, 1401–05 (2014) (arguing that autonomous weapons cannot satisfy IHL's accountability structure unless human responsibility remains central, particularly in decisions involving the use of lethal force).

212. Priya Mondal et al., *Bridging the Gap: Artificial Intelligence in Addressing the Accountability Gap in International Humanitarian Law*, 13 Frontiers in Health Informatics 7933 7935–38 (2024) (explaining how IHL's emphasis on human and state responsibility informs emerging proposals for algorithmic-governance frameworks aimed at resolving accountability gaps created by AI systems).

213. Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, U. Ill. J. L. Tech. & Pol'y 239, 265–68 (2007) (arguing that legal systems depend on identifiable human responsibility and oversight to adapt effectively to technological change).

214. *See generally* Dimitri Van Den Meerssche, *Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association*, 33 Eur. J. Int'l L. 171, 188–92 (2022) (arguing that fragmented U.S., EU, and international legal regimes create accountability gaps in algorithmic governance and require cross-jurisdictional coordination).

215. Annelise Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, 47 Cornell Int'l L. J. 63 70–76 (2014) (explaining how regulatory arbitrage enables actors to evade stricter domestic regimes and threatens the stability of underlying legal norms, thereby underscoring the need for frameworks that close both domestic and cross-border accountability gaps).

foreign policy.[216] They offer tested mechanisms such as sectoral carve-outs, meaningful human control, and rigorous impact assessments, that can inform the ongoing refinement of U.S. law while reminding policymakers of the enduring challenges of balancing national security with the rule of law.[217]

IV. Algorithmic Interventions: Illustrative Cases

Recent innovations in AI have not merely introduced new technical capabilities to foreign relations and national security, but have fundamentally reconfigured the operational and legal landscape in which the state exercises power.[218] The following case studies illuminate how algorithmic systems are already reshaping core domains, ranging from the deployment of autonomous drones to the transnational sharing of AI-augmented surveillance data to the use of large language models in the negotiation and drafting of diplomatic texts. This section highlights the doctrinal ambiguities, accountability gaps, and constitutional risks that arise from the practical integration of AI into high-stakes government decision-making. These real-world contexts underscore the pressing need for reimagined legal guardrails and enhanced institutional oversight in the era of algorithmic governance.

A. Autonomous Drone Strikes and Executive Agreements on Use of Force

The increasing reliance on autonomous drone systems for targeted strikes has fundamentally altered the architecture of American use-of-force decision-making, exposing acute doctrinal and practical gaps in legal accountability.[219] At the operational level, contemporary drone strikes often involve a "decision chain" in which algorithms conduct real-time surveillance, select targets, and initiate force with minimal human intervention.[220] Executive agreements with host states or coalition partners, often classified and negotiated without legislative involvement, further complicate the accountability structure, functioning as de facto authorizations of military action outside the framework of public international law or express congressional approval.[221]

---

216. Artur Ishkhanyan, *The Sovereignty-Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control*, 5.1 Discover Artificial Intelligence 123, 134–39 (2025) (explaining how divergent national approaches to AI governance create structural barriers to transnational accountability while demonstrating the need for internationally coordinated oversight).

217. Ünver, *supra* note 71, at 9-12.

218. Sertaç *supra* note 14, at 88-90.

219. Diane M. Vavrichek, *The Future of Drone Strikes: A Framework for Analyzing Policy Options,* Center for Naval Analyses, 46, 46–49 (2014) (assessing how increasing automation in drone-strike systems reshapes U.S. use-of-force decision processes and generates significant accountability gaps).

220. Sviatoslav Vasylyshyn & Ivan Opirskyy, *Combat Drone Swarm System (CDSS) Based on Solana Blockchain Technology* 4–7 (Seventh Int'l Workshop on Computer Modeling and Intelligent Systems, 2024) (describing autonomous drone-swarm architectures in which algorithms perform surveillance, target selection, and coordinated strike actions with minimal human involvement).

221. *See generally* David Wippman, *Military Intervention, Regional Organizations, And Host-State Consent,* 7 Duke J. Comp. & Int'l L. 209, 211-212 (1996) (explaining how host-state

A close legal analysis of these operational frameworks reveals several layers of concern. First, the delegation of target selection and strike initiation to machine learning algorithms raises unresolved questions about compliance regarding domestic constitutional constraints and international humanitarian law.[222] The lack of statutory clarity regarding what constitutes "meaningful human control" allows executive agencies to develop their own interpretations, often shielded from judicial or legislative review.[223] The executive's reliance on AI-enabled weapons exacerbates the accountability deficits endemic to the contemporary war powers regime, particularly where operational details are obscured by classification or nonpublic executive agreements.[224]

Second, the very structure of these executive agreements often bypasses the statutory guardrails envisioned by the War Powers Resolution and related legislation. With the proliferation of informal or secret memoranda of understanding regarding drone basing, operational parameters, and permissible targets, Congress is effectively sidelined from both the initiation and oversight of hostilities.[225] Judicial intervention is similarly rare, with courts invoking doctrines of nonjusticiability or political questions to avoid entanglement in operational details, an avoidance amplified by the technological opacity of autonomous weapons systems.[226]

Finally, the absence of effective statutory or judicial oversight allows for a problematic diffusion of responsibility in the event of error or collateral damage.[227] When strike decisions originate in algorithmic inference engines, operating according to proprietary, nontransparent code, the question of who

---

consent agreements can operate as functional authorizations for military action outside formal treaty processes and without legislative oversight).

222. *See, e.g.*, Mahshad Jafariandehkordi, The AI Battlefield: *Legal Challenges of Autonomous Weapon Systems Under International Humanitarian Law* 31–45 (2024) (Master's Thesis, Åbo Akademi University), *available at* https://www.doria.fi/bitstream/handle/10024/189724/jafariandehkordi_mashad.pdf?sequence=3&isAllowed=y [https://perma.cc/3KZJ-8UED] (analyzing how machine-learning-driven target selection and strike initiation create unresolved compliance challenges under IHL and complicate responsibility assessments).

223. Herman Veluwenkamp, *Reasons for Meaningful Human Control*, 24 Ethics and Info. Tech. 51, 57–60 (2022) (explaining that the absence of a consistent definition of "meaningful human control" allows institutions to construct their own interpretations, creating accountability gaps and limiting external oversight).

224. *See generally* Mehmet Emin Erendor, *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons* 143–51 (CRC Press 2024) (explaining how AI-enabled and autonomous weapons systems expand executive discretion, reduce transparency, and create accountability gaps in national-security decision-making).

225. Milena Sterio, *The Covert Use of Drones: How Secrecy Undermines Oversight and Accountability*, 8 Alb. Gov't L. Rev. 129, 138–43 (2015) (explaining that secret drone agreements with host states and undisclosed operational rules prevent Congress from exercising meaningful war-powers oversight).

226. Benjamin Kastan, *Autonomous Weapons Systems: A Coming Legal " Singularity"?*, U. Ill. J. L. Tech. & Pol'y 45, 67–72 (2013) (explaining that courts are likely to avoid adjudicating disputes involving autonomous weapons by invoking political question and nonjusticiability doctrines, especially given the opacity and technical complexity of such systems).

227. Noah Rahimzadagan et al., *Drone Fail Me Now: How Drone Failures Affect Trust and Risk-Taking Decisions* 6-10 (2024 ACM/IEEE International Conf.on Human-Robot Interaction, (2024) (showing that failures in autonomous drone systems create fragmented perceptions of responsibility, illustrating how accountability diffuses when oversight mechanisms are weak).

is legally accountable becomes clouded.[228] Unfortunately, the existing legal framework fails to map responsibility onto the actual decision-makers, human or machine, enabling a culture of impunity in the exercise of lethal force.

In summary, the case of autonomous drone strikes highlights the need to develop legal frameworks that can effectively reassert congressional and judicial oversight over the use of military force in the AI era. Without such guardrails, the constitutional and humanitarian risks posed by algorithmic targeting will remain acute, undermining both democratic legitimacy and the foundational principles of international law.

B. AI-Augmented Surveillance and Data-Sharing Agreements

The proliferation of AI-powered surveillance has transformed the landscape of transnational intelligence cooperation, especially among members of the Five Eyes alliance and similar intelligence-sharing partnerships.[229] These arrangements increasingly rely on advanced machine learning systems, ranging from facial recognition platforms to behavioral prediction engines, to process, analyze, and interpret massive volumes of cross-border data.[230] The rise of AI inference engines raises profound legal and constitutional concerns, particularly regarding privacy, sovereignty, and the adequacy of existing oversight mechanisms.[231]

At the heart of contemporary data sharing agreements is the deployment of AI tools capable of inferring sensitive information from disparate datasets, often at a scale and speed beyond the reach of traditional human analysts.[232] Agreements between intelligence partners routinely permit the pooling and algorithmic processing of data streams, blurring the lines between domestic and foreign intelligence operations.[233] AI-enhanced surveillance technologies both expand the scope of intelligence gathering and undermine traditional

---

228. Anthony Downey, *Algorithmic Predictions and Pre-emptive Violence: Artificial Intelligence and the Future of Unmanned Aerial Systems*, 5 Digit. War 123, 131–35 (2024) (explaining how opaque, proprietary algorithmic systems embedded in drone platforms obscure responsibility for predictive or pre-emptive strike decisions).

229. *See generally* Karwan Mustafa Kareem, *The Cyber Eye: Inside the Network Wars and Secrets of the Five Eyes Alliance* 112–18 (Lulu Press, Inc. 2025) (describing how AI-enabled surveillance and data-analytics systems have reshaped intelligence-sharing practices and operational cooperation within the Five Eyes alliance).

230. Anastasios Nikolaos Kanellopoulos, *Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges*, 3.1 J. Pol. & Ethics New Tech. & AI 1, 12–18 (2024) (examining how facial-recognition systems, behavioral-prediction algorithms, and other machine-learning tools process and analyze large-scale intelligence data across borders).

231. Rama Dutt, *AI and the Right to Privacy - Balancing Innovation with Constitutional Protections*, 3 LawFoyer Int'l J. Doctrinal Legal Rsch. 920, 927–33 (2025) (explaining how AI inference engines threaten constitutional privacy rights, complicate sovereign control over data governance, and expose deficiencies in existing oversight mechanisms).

232. Abdul Majeed & Seong Oun Hwang, *When AI Meets Information Privacy: The Adversarial Role of AI in Data Sharing Scenario*, 11 IEEE Access 76177, 76182–87 (2023) (showing that AI systems can infer sensitive information by integrating disparate datasets and operating at analytic scales far exceeding human capabilities).

233. Rachel C. Taylor, *Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State*, 17 Wash. U. Global Stud. L. Rev. 731, 744–52 (2018) (explaining how multilateral intelligence-sharing arrangements permit pooled and

jurisdictional safeguards, creating new vulnerabilities for individual rights and state accountability.[234]

The opacity of algorithmic inference, coupled with the secretive nature of executive agreements governing intelligence cooperation, has frustrated meaningful legislative and judicial review.[235] Congressional committees often receive only summary disclosures of technical capabilities or broad assurances of compliance with statutory standards, while the underlying mechanisms of AI analysis, such as neural network weights or decision-tree logic, remain shielded as classified or proprietary.[236] Judicial review is more rare, as courts defer to executive assessments of national security and invoke the "state secrets doctrine" to bar litigation.[237] The resulting accountability gap is especially acute for cross-border data flows, where allied states or third parties conduct surveillance abroad that can circumvent domestic legal protections and oversight.[238]

Recent incidents underscore the risks. For example, revelations of mass surveillance programs involving Five Eyes partners and the use of AI for bulk metadata analysis have triggered legal challenges in multiple jurisdictions, highlighting persistent ambiguities around consent, minimization, and proportionality requirements.[239] The lack of harmonized standards for algorithmic decision-making and data retention exacerbates the risk of rights violations, while leaving key aspects of these arrangements outside the reach of domestic and international law.[240]

---

algorithmically processed data streams that blur distinctions between domestic and foreign intelligence activities).

234. Vanshika Jain & Rekha Verma, *Governing the Artificial Intelligence of Things: Navigating Techno-Legal Challenges in a Connected World* 14–22 (SSRN Working Paper, Paper No. 5254579, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5254579 [https://perma.cc/M4XP-T67G] (explaining how AI-enhanced, networked surveillance systems expand intelligence-gathering capacity while weakening jurisdictional safeguards and increasing risks to individual rights and governmental accountability).

235. Bukunmi Temiloluwa Ofili et al., *Securing US National Interests with Cloud Innovation: Data Sovereignty, Threat Intelligence and Digital Warfare Preparedness*, 12 Int'l J. Sci. Rsch. Archive 3160, 3167–73 (2024) (explaining how opaque AI-driven threat-intelligence systems and confidential data-sharing arrangements limit transparency and hinder external oversight).

236. *See* Gordon Unzen, *Artificial Intelligence and the Administrative State: Regulating the Government Use of Decision-Making Technology*, 25 Minn. J.L. Sci. & Tech. 209, 234–38 (2023) (noting that congressional oversight often relies on high-level summaries because agencies withhold underlying AI model architecture, decision logic, and proprietary or classified technical details).

237. *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 Geo. Wash. L. Rev. 1249, 1308–12 (2006) (discussing how courts defer to executive national-security judgments and routinely invoke the state secrets doctrine to bar litigation, thereby limiting judicial review).

238. *See* Jatish Gulia, *Cross-Border Data Transfers: International Cooperation and Conflicts*. 4 Legal Lock J. 263, 273–77 (2024) (explaining how international data-transfer arrangements can allow states to evade domestic privacy safeguards and weaken accountability when surveillance is routed through foreign partners).

239. *See* Wenli Yang, et al., *The Impact and Influence of Modern AI in Metadata Management*, 5 Hum.-Centric Intelligent Sys. 323, 331–37 (2025) (describing how AI-driven bulk metadata analysis expands surveillance capabilities and generates privacy concerns relating to consent, minimization, and proportionality).

240. *See generally* Elham Torkaman & Kaveh Ranjbaran, *Indicators of Human Rights Risks in Automated Decision-Making Systems*, 2.2 J. of Hum. Rts. L. & Poli'y 1, 4–7 (2024)

In conclusion, the legal frameworks that govern AI-augmented surveillance and data sharing must evolve to address both technological complexity and the transnational character of intelligence operations. This includes greater transparency in executive agreements, meaningful technical disclosures to legislative bodies, and the development of joint oversight mechanisms that span national borders.[241] Without such reforms, the convergence of AI, surveillance, and cross-border data flow threaten to erode foundational norms of accountability and democratic control.

C. Predictive Diplomacy and Natural Language AI in Negotiation

The introduction of LLMs and predictive AI tools into the sphere of diplomatic negotiation is a significant departure from traditional models of statecraft. These systems, capable of drafting, simulating, and interpreting complex diplomatic positions, have begun to inform the strategies of both national governments and international organizations.[242] While the allure of greater efficiency and strategic insight is undeniable, the deployment of LLMs in diplomatic contexts raises a host of legal and normative concerns regarding transparency, textual authorship, and accountability.[243] At their core, LLMs enable diplomats to rapidly generate or simulate negotiating positions, predict responses from counterparts, and analyze voluminous treaty language or historical records.[244] Governments are increasingly turning to these tools to anticipate the likely consequences of policy stances, optimize communication strategies, and even produce draft language for bilateral or multilateral agreements.[245]

However, the reliance on AI-generated text complicates questions of attribution and responsibility under international law. This is due to the opacity and speed of algorithmic reasoning and textual generation, which risks obscuring the identity of accountable state actors.[246] This opacity is particularly problematic in the context of international legal commitments, where the

(explaining how fragmented algorithmic-governance standards and weak data-retention rules heighten human-rights risks and leave major aspects of automated decision-making outside effective legal oversight).

241. *See* Bradley & Morrison, *supra* note 124, at 1120–27.

242. *See* Marta Konovalova, *AI and Diplomacy: Challenges and Opportunities*, 9 J. Liberty & Int'l Affs. 520, 526–31 (2023) (discussing how governments and international organizations are using AI systems to draft and simulate diplomatic positions, marking a significant shift from traditional diplomatic practice).

243. *See generally* Princy Pappachan, et al.,*Transparency and Accountability*, *in* Challenges in Large Language Model Development and AI Ethics 178, 182–87 (2024) (explaining how LLM opacity, unclear textual authorship, and responsibility gaps pose significant legal and normative challenges for institutional uses of LLM-generated content).

244. *See* Muneera Bano, et al., The Role of Generative AI in Global Diplomatic Practices: A Strategic Framework 6–12 (unpublished manuscript) (2023), *available at* https://arxiv.org/pdf/2401.05415 [https://perma.cc/LT7J-2BHD] (describing how LLMs assist diplomats in generating and simulating negotiating positions, predicting counterpart responses, and analyzing extensive treaty and historical texts).

245. *See* Sadegh-Zadeh *supra* note 46, at 70-72.

246. Bérénice Boutin, *State Responsibility in Relation to Military Applications of Artificial Intelligence*, 36 Leiden J. Int'l L. 133, 133–38 (2023) (explaining how the opacity and automation of AI systems complicate the attribution of conduct to states, thereby challenging traditional responsibility frameworks).

precise meaning and provenance of treaty language can be determinative.[247] Automated drafting and simulation can create ambiguities about the intentions of parties, the binding nature of negotiated terms, and the identification of "travaux préparatoires" or preparatory work that may be critical to later interpretation.[248] When diplomats rely on text produced by LLMs, it can be uncertain whether states truly comprehend or intend the legal implications of their commitments, which is heightened by the technical complexity of these models, and the risk that they may generate inaccurate or misleading content, commonly referred to as "hallucinations."[249]

Another challenge to transparency is the confidential and classified nature of diplomatic negotiation. The integration of LLMs, especially those developed or trained by private entities, introduces risks of data leakage, model bias, and inadvertent exposure of sensitive national positions.[250] Ensuring proper documentation, audit trails, and verifiable attribution becomes both more important and more difficult in the age of predictive diplomacy.[251] The absence of clear technical and procedural safeguards may call into question the legitimacy of international agreements, and disputes over interpretation or attribution are likely to proliferate.[252]

In essence, this Article proposes that the emerging use of LLMs in diplomacy demands a recalibration of both legal doctrine and institutional practice. Building on recommendations from recent scholarship, regulatory and treaty frameworks will need to require rigorous documentation of AI involvement in negotiation, mandate human verification of all substantive commitments,

---

247. Matthijs M. Maas, *International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order*, 20 Melb. J. Int'l L. 29, 54–60 (2019) (explaining how AI opacity obscures authorship, intent, and interpretive provenance, thereby threatening the clarity and determinacy required for treaty obligations).

248. *See generally* William A. Schabas, The Universal Declaration of Human Rights: The Travaux Préparatoires 15–22 (Cambridge University Press ed. 2013) (demonstrating how preparatory records illuminate state intent and the meaning of negotiated text, underscoring why AI-generated drafting risks obscuring the interpretive materials essential for treaty analysis).

249. *See* Jim Waldo and Soline Boussard, *GPTs and Hallucination: Why Do Large Language Models Hallucinate?* 68 Commc'ns ACM 19, 21–25 (2024) (explaining that LLMs often produce inaccurate or fabricated text due to their probabilistic design and internal opacity, raising concerns when such content is relied on in high-stakes contexts).

250. Vishal Rathod, et al. *Privacy and Security Challenges in Large Language Models 4-9* (2025 IEEE 15th Ann. Computing and Commc'n Workshop and Conf., 2025) (identifying risks of data leakage, bias, and exposure of sensitive information when LLMs—especially privately developed or externally hosted models—are used in governmental or strategic contexts).

251. *See generally* Nicolin Decker, *The Doctrine of Strategic Restraint: A Framework for Diplomatic De-escalation and Global Escalation Prevention Integrating Moral Forecasting, Conflict Modeling, and Systems Stewardship for 21st-Century Statecraft* 28–34 (SSRN Working Paper, Paper No. 5320166, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5320166 [https://perma.cc/932E-86RJ] (explaining how AI-enhanced, networked surveillance systems expand intelligence-gathering capacity while weakening jurisdictional safeguards and increasing risks to individual rights and governmental accountability).

252. *See* Mauricio Baker, *Nuclear Arms Control Verification and Lessons for AI Treaties* 7–13 (unpublished manuscript, 2023), *available at* https://arxiv.org/abs/2304.04123 [https://perma.cc/2Z7U-LTSS] (arguing that insufficient technical and procedural safeguards undermine treaty legitimacy and lead to interpretation and attribution disputes, a dynamic likely to recur in AI governance agreements).

and facilitate independent review of algorithmic contributions to international legal texts. Without such reforms, the convergence of AI and diplomacy risks eroding not only the clarity of international law but also the foundations of trust and accountability upon which effective global governance depends.

V. Toward a Legally Responsible Algorithmic State

The acceleration of AI in foreign relations presents a critical inflection point for American constitutionalism. As state actors increasingly deploy automated systems in diplomacy, security, and the exercise of sovereign power, the boundaries of legal oversight and executive discretion are rapidly shifting.[253] The challenge is not simply one of technical adaptation, but of legal and democratic recalibration: how can state actors preserve foundational principles of transparency, accountability, and human judgment when machines play a decisive role in high-stakes decision-making? This section addresses the core question of how to construct a legally responsible algorithmic state that establishes principled constitutional thresholds for the deployment of AI in foreign affairs. The section also outlines a legislative blueprint to ensure that technological progress does not erode the constitutional foundations of American governance.

A first-order imperative is to define constitutional thresholds for permissible algorithmic use in foreign relations and national security, given that not all state action can be entrusted to machines.[254] Certain categories of decision-making, such as the initiation of war, the binding of the nation through treaties, and the assertion or waiver of fundamental rights, must remain the exclusive province of accountable human actors.[255] Legislation and executive policy must draw clear lines that bar autonomous AI from making irrevocable sovereign commitments, and provide for robust, human-in-the-loop oversight wherever algorithmic systems are deployed.

Beyond categorical exclusions, future statutory frameworks should articulate functional and procedural constraints tailored to the distinctive challenges of algorithmic governance.[256] These should include dynamic review

253. Cary Coglianese, *Administrative Law in the Automated State*, 150 Daedalus 104, 112–15 (2021) (explaining how automation expands executive capacity and strains traditional mechanisms of constitutional oversight, a dynamic that parallels the increasing use of AI in diplomacy and national-security decision-making).

254. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev 1, 24–31 (2003) (arguing that automated analytic tools used for national-security purposes must operate within constitutional limits, underscoring the need to define permissible thresholds for algorithmic state action).

255. *See* David Leslie, et al., *The Alan Turing Institute, Artificial Intelligence, Human Rights, Democracy, and the Rule of Law: A Primer* 22–30 (The Alan Turing Institute 2021) (emphasizing that sovereign acts affecting war powers, treaty obligations, and fundamental rights require accountable human decision-makers because AI systems cannot satisfy democratic or rule-of-law requirements).

256. *See* Pedro Rubim Borges Fortes, et al., *Artificial Intelligence Risks and Algorithmic Regulation*, 13 Eur. J. Risk Reg. 357, 370–78 (2022) (arguing that effective AI governance requires adaptive oversight, traceability, mandatory documentation, and enhanced judicial and legislative review mechanisms).

mechanisms keyed to the level of autonomy exercised by AI systems, mandatory documentation and reporting requirements, and expanded opportunities for judicial and congressional scrutiny.[257] Drawing from both comparative experience and normative theory, lawmakers should require that all algorithmic action in foreign relations be subject to ex ante and ex post evaluation. This would ensure both transparency and the possibility of redress in the event of error or abuse.

A blueprint for responsible algorithmic statecraft must also address the risk of regulatory arbitrage and the diffusion of accountability across borders. A coordinated legislative response, informed by the adaptation of international legal standards, can prevent the erosion of democratic control and the circumvention of constitutional safeguards.[258] This will require the modernization of existing instruments such as the War Powers Resolution and the International Emergency Economic Powers Act, as well as the enactment of new statutory regimes specifically designed for the age of AI.[259]

Ultimately, the emergence of the algorithmic state is not merely a technical evolution but a constitutional reckoning.[260] The promise of AI in advancing the effectiveness and precision of foreign policy cannot be realized without corresponding legal innovation to ensure that the core values of transparency, accountability, and human judgment endure.[261] Only by embracing a framework of legally responsible algorithmic governance can the United States preserve its constitutional order and democratic legitimacy in a rapidly changing world.

A. Reimagining Foreign Relations Law for Automated Decision-Making

The integration of AI into executive foreign relations demands a fundamental reassessment of longstanding doctrinal assumptions within U.S. foreign relations law. Historically, the constitutional structure has relied upon the premise that foreign affairs are entrusted to politically accountable officials, guided by established legal and procedural checks that assume human discretion, deliberation, and intent.[262] The rapid adoption of algorithmic tools in diplomatic,

257. *Id.* at 370-76.

258. Kevin L. Cope & Mila Versteeg, *The Procedure of Democratic Erosion*, 73 Emory L.J. 1249, 1264-68 (2023-2024) (explaining how institutional fragmentation, procedural gaps, and cross-border dynamics enable accountability evasion and undermine democratic safeguards, underscoring the need for coordinated legal standards).

259. *See generally* Timothy Meyer & Ganesh Sitaraman, *The National Security Consequences of the Major Questions Doctrine*, 122 Mich. L. Rev. 55, 57-60 (2023) (arguing that existing national-security statutes are ill-equipped for modern technological contexts and that congressional modernization is required to govern emerging executive practices).

260. *See generally* Oreste Pollicino & Giovanni De Gregorio, *Constitutional Law in the Algorithmic Society*, *in* Constitutional Challenges in the Algorithmic Society 15, 18–24 (Cambridge University Press 2021) (arguing that algorithmic governance transforms core constitutional principles, requiring a rethinking of rights protections, accountability, and democratic control).

261. *See* Hazrat Usman, Iqra Tariq, & Bushra Nawaz, *In the Realm of the Machines: AI's Influence Upon International Law and Policy*, 4 J. Soc. Rsch. Dev. 383, 390-94 (2023) (arguing that AI's potential to strengthen foreign-policy decision-making depends on legal reforms that preserve transparency, accountability, and human oversight).

262. Kim Lane Scheppele, *Restoring Democracy Through International Law*, 39 Am. U. Int'l L. Rev. 587, 594–602 (2024) (explaining that constitutional democracies rely on

military, and intelligence settings challenges these foundational presumptions by introducing opaque, non-human agents into processes that implicate war powers, treaty obligations, and the core prerogatives of sovereignty.[263]

As recent executive practices demonstrate, delegating critical foreign policy functions to machine-learning models or autonomous systems may bypass the anticipated mechanisms of democratic accountability, such as public justification, congressional oversight, or judicial review.[264] This technological shift heightens the risk that executive agreements or operational protocols may produce binding commitments or kinetic outcomes without meaningful deliberation or remedy—effectively widening the gap between executive power and legal responsibility.[265]

To maintain the legitimacy of U.S. foreign relations law in this emerging context, courts and lawmakers must reexamine foundational principles with a focus on the unique affordances and perils of automated decision-making.[266] The legal meanings of discretion, intent, and responsibility must be recast to reflect both the technical opacity of advanced algorithmic systems and the persistent need for human oversight.[267] This reframing requires not only doctrinal innovation but also an ongoing dialogue among all three branches of government to adapt procedural safeguards, oversight mechanisms, and substantive constitutional thresholds for the age of algorithmic governance. Recent commentary has underscored the urgency of this task. The growth of algorithmic governance in national security heightens the stakes of the accountability gap that already challenges executive power.[268]

The next generation of foreign relations law must thus engage directly with the question of how the law will respond to non-human actors that execute or even shape the nation's international commitments and operations.[269]

---

politically accountable human actors, operating under procedural and legal checks, to conduct foreign affairs).

263. Shayne Longpre, Marcus Storm & Rishi Shah, *Lethal Autonomous Weapons Systems & Artificial Intelligence: Trends, Challenges, and Policies*, 3 MIT Sci. Pol'y Rev. 47, 56-58 (2022) (describing how opaque and increasingly autonomous AI systems in military and intelligence contexts displace traditional human oversight and raise challenges for accountability, sovereignty, and war-powers decision-making).

264. *See* Wrap Up: Congress Must Ensure the Federal Government Has Tools to Deploy Artificial Intelligence Effectively and Efficiently, U.S. House Comm. on Oversight & Accountability (June 6, 2025), https://oversight.house.gov/release/wrap-up-congress-must-ensure-the-federal-government-has-tools-to-deploy-artificial-intelligence-effectively-and-efficiently/ [https://perma.cc/GQD6-28BQ] (warning that executive agencies are deploying AI systems in ways that may evade congressional oversight, transparency).

265. Kathleen Claussen, *The Improvised Implementation of Executive Agreements*, 89 U. Chi. L. Rev. 1655, 1664–72 (2022) (explaining that executive agreements are often implemented through opaque, informal processes that produce binding foreign-policy commitments without meaningful oversight or remedies, thereby creating accountability gaps).

266. *Id.* at 1668–75.

267. Frosio, *supra* note 184.

268. Kristen Eichensehr, *The Youngstown Canon: Vetoed Bills and the Separation of Powers*, 70 Duke L.J. 1245, 1280–89 (2021) (explaining the structural accountability deficits in modern executive power, particularly in national security, which algorithmic governance threatens to exacerbate).

269. *See, e.g.*, André Nunes Chaib, *Multinaturalism in International Environmental Law: Redefining the Legal Context for Human and Non-Human Relations*, 12 Asian J. Int'l L. 82, 95–101 (2022) (arguing that international law must adapt to account for non-human actors

Only by recentering legal frameworks around the realities of algorithmic decision-making can constitutional law ensure that the exercise of power in foreign affairs remains both effective and accountable.

B. Defining Constitutional Thresholds for Permissible Algorithmic Use

The constitutional permissibility of algorithmic decision-making in foreign relations must be situated within established doctrines while recognizing the distinct challenges posed by AI.[270] The Supreme Court's separation of powers jurisprudence, especially in cases addressing executive discretion and nondelegation, presupposes human judgment, context-sensitive reasoning, and the possibility of direct accountability.[271] The migration toward autonomous or semi-autonomous algorithmic systems, complicates the application of foundational constitutional tests and necessitates the development of new analytic thresholds to govern the use of AI in matters implicating foreign affairs.[272]

First, any algorithmic tool deployed in the context of executive agreements or national security must be subject to a nondelegation analysis that recognizes the qualitative differences between human and machine judgment.[273] While the intelligible principle doctrine has traditionally permitted broad delegations to executive agencies, the opacity and unpredictability of algorithmic systems may undermine the premises of meaningful guidance or constraint.[274] As recent scholarship has argued, the "black box" nature of many machine learning systems challenges efforts to ensure that executive branch actors retain ultimate responsibility for policy outcomes.[275]

---

that influence legal processes, offering an analogue for how foreign-relations law should respond to AI systems that shape or execute state commitments).

270. Ryan David Kiggins, *Big Data, Artificial Intelligence, and Autonomous Policy Decision-Making: A Crisis in International Relations Theory?*, *in* The Political Economy of Robots 211, 218–24, (Ryan Kiggins ed., 2018) (explaining how AI and autonomous systems disrupt traditional governance assumptions, illustrating why established doctrines must be reassessed to address the distinct challenges posed by algorithmic decision-making).

271. Matthew James Tanielian, *Separation of Powers and the Supreme Court: One Doctrine, Two Visions*, 8 Admin. L.J Am. U. 961, 972–80 (1994) (describing how the Court's separation-of-powers and nondelegation doctrines assume human discretion, context-based reasoning, and identifiable accountability—assumptions unsettled by algorithmic decision systems).

272. Eric Tjong Tjin Tai, *Liability for (Semi) Autonomous Systems: Robots and Algorithms*, *in* Research Handbook on Data Science And Law (Edward Elgar 1st ed. 2018) (explaining how autonomous and semi-autonomous systems undermine traditional legal assumptions of human agency and control, demonstrating why new analytic thresholds are needed when applying existing doctrines to AI-driven decision-making).

273. Tjerk de Greef, *Delegation and Responsibility: A Human–Machine Perspective, in* Drones and Responsibility 134, 138–44 (Routledge 1st ed. 2016) (explaining why delegating authority to machines differs fundamentally from delegating to humans, thereby supporting the need for a distinct nondelegation analysis when algorithms exercise national-security or foreign-affairs functions).

274. Moto Kamiura, *The Four Fundamental Components for Intelligibility and Interpretability,* 62 Am. Philos. Q. 103, 109–15 (2025) (explaining how opacity and non-interpretability in AI systems impede meaningful human guidance and oversight, thereby challenging assumptions underlying the intelligible-principle doctrine).

275. Jennifer Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making,* 39 Legal Stud. 636, 642–49 (2019) (explaining how the opacity of machine-learning systems undermines traditional mechanisms for ensuring executive responsibility and accountability for governmental decisions).

Second, constitutional thresholds for permissible use must be grounded in robust oversight and transparency requirements. Where executive agreements or operational directives incorporate algorithmic recommendations, the processes by which inputs are selected, outputs are validated, and errors are addressed should be subject to both congressional and judicial scrutiny.[276] This is especially critical in domains, such as the use of force or surveillance, where algorithmic decisions may have direct and irreversible consequences for fundamental rights and the nation's international obligations.

Third, courts and policymakers must assess whether algorithmic decision-making is compatible with procedural due process and equal protection guarantees. When AI-informed foreign policy actions affect individual rights or create disparate impacts, the Constitution requires that affected persons receive meaningful notice, explanation, and opportunity for redress.[277] The tendency of certain AI systems to replicate or amplify bias heightens the importance of constitutional scrutiny at every stage of their deployment.

Defining these constitutional thresholds is not simply an exercise in doctrinal adaptation; it is a normative commitment to ensuring that advances in executive capacity do not outpace the development of safeguards essential to democratic legitimacy.[278] As algorithmic governance becomes embedded in the conduct of U.S. foreign relations, the Constitution must serve both as a boundary and a guide, establishing conditions for innovation that preserve the core principles of accountability, transparency, and human dignity.[279]

C. Blueprint for Future Legislation and Executive Constraints

The emergence of algorithmic systems in foreign relations compels lawmakers and executive officials to design legislative and regulatory structures that harness technological innovation while upholding the rule of law. Given the transformative potential and inherent opacity of AI-driven tools, the traditional checks and balances that have defined U.S. governance must be recalibrated to address new vectors of risk, ranging from diminished transparency to weakened accountability in matters of war, diplomacy, and transnational surveillance.[280]

---

276. David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 Yale J. on Reg. 800, 827–28 (2020) (arguing that governmental use of algorithms requires transparency, documentation, and mechanisms for oversight and error correction, enabling both legislative and judicial scrutiny).

277. *See, e.g.*, Alfred Hill, *Constitutional Remedies*, 69 Colum L. Rev. 1109, 1112–14 (1969) (explaining that constitutional guarantees of due process and equal protection require meaningful notice, explanation, and access to remedies for individuals affected by government action, principles that apply when algorithmic systems shape foreign-policy decisions).

278. *See* Mariano-Florentino Cuéllar, *From Doctrine to Safeguards in American Constitutional Democracy*, 65 UCLA L. Rev. 1398, 1415–16 (2018) (arguing that constitutional legitimacy depends on developing safeguards that evolve alongside expanding executive capacity, reinforcing the need for normative limits on new technologies such as algorithmic decision-making).

279. *See generally* Coglianese & Lehr, *supra* note 143.

280. Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 Berkley Tech L.J. 773 799–808 (2019) (explaining how the

A legislative blueprint for the algorithmic age should begin with statutory requirements for transparency and explainability in executive use of AI. Congress should mandate that all algorithmic systems employed in the context of executive agreements, military operations, or foreign intelligence be subject to meaningful documentation, regular auditing, and public reporting, where national security interests permit.[281] These measures are not only necessary to enable congressional oversight but also to foster public trust and to provide courts with a record upon which to evaluate constitutional claims.

Furthermore, statutory reforms should establish procedural safeguards to limit the delegation of sensitive foreign policy decisions to algorithmic systems. These may include mandatory human-in-the-loop requirements for the authorization of kinetic or surveillance operations, independent review boards to assess compliance with constitutional and statutory norms, and limitations on the executive's ability to invoke secrecy in withholding algorithmic protocols from meaningful oversight.[282] Legislation should also provide explicit mechanisms for redress and remedial action where algorithmic error, bias, or malfunction produces adverse effects, particularly where individual rights or international commitments are implicated.[283]

Finally, executive self-restraint must be institutionalized through revised internal guidelines and executive orders. Agencies involved in foreign affairs should develop detailed protocols for the ethical and legal deployment of AI, drawing on best practices from comparative jurisdictions and international organizations. These protocols should articulate clear lines of responsibility, establish criteria for algorithmic validation and monitoring, and ensure that decision-making authority ultimately rests with accountable human officials.

As algorithmic systems become increasingly embedded in the conduct of U.S. foreign relations, only a comprehensive legislative and regulatory approach can ensure that the benefits of technological innovation are realized without eroding the constitutional architecture that underpins democratic governance. A forward-looking statutory framework, grounded in transparency, oversight, and human accountability, is essential to reconcile the imperatives of national security with the enduring demands of constitutional order.

---

opacity and systemic risks of machine-learning tools undermine traditional mechanisms of transparency and accountability, demonstrating the need to recalibrate governmental checks and balances when agencies adopt AI).

281. Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 Fla. L. Rev. 1045, 1083–89 (2016) (arguing that algorithmic intelligence systems require robust documentation, auditing, and reporting mechanisms to ensure effective congressional and judicial oversight and to mitigate accountability deficits).

282. *See, e.g.*, Hannah Bloch-Wehba, *Algorithmic Governance from the Bottom Up*, 48 BYU L. Rev. 69, 110–18 (2022) (arguing that algorithmic decision-making by government actors requires procedural safeguards—including transparency, independent review, and mechanisms preserving human authority—to prevent accountability erosion).

283. Nathalie A. Smuha, *Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea*, 34 Phil. & Tech. 91, 108–12 (2021) (arguing that effective AI regulation requires robust accountability and redress mechanisms to address harms arising from algorithmic error, bias, or malfunction).

Conclusion

The rise of artificial intelligence as a core component of U.S. foreign policy and national security is more than a technological evolution. It is a profound legal and constitutional challenge.[284] This Article has demonstrated that the diffusion of algorithmic tools into the core of executive decision-making, from the negotiation of international agreements to the use of force and the conduct of diplomacy, undermines the legal doctrines that have long guided and restrained the exercise of state power. While the promise of increased efficiency, predictive capability, and data-driven insight is undeniable, so too is the risk that foundational principles, such as transparency, human accountability, and separation of powers, will be subordinated to the imperatives of technological expedience.[285]

The doctrinal gaps exposed by the deployment of AI in executive agreements and military operations demand urgent legal and institutional innovation. Key constitutional and statutory mechanisms, including the War Powers Resolution, the nondelegation doctrine, and the political question doctrine, all presume human agency and observable decision-making.[286] In an era when algorithmic processes can obscure the origin and rationale of critical foreign policy actions, these doctrines no longer offer reliable guardrails for democratic accountability or effective oversight.

To address these challenges, Congress should enact legislation that specifically addresses the use of AI and autonomous systems in foreign relations and national security decision-making. Such legislation should require transparent reporting to Congress regarding any executive agreements or military actions substantially informed or executed by algorithmic systems, including the rationale, scope, and oversight mechanisms for such use.[287] The executive branch should be obliged to notify Congress not only when U.S. forces are introduced into "hostilities" (as currently required under the War Powers Resolution), but also when autonomous or AI-enabled systems are used in kinetic or cyber operations with the potential for escalation or legal ambiguity.[288] There is also a clear need for an independent, cross-agency oversight body, staffed by technical and legal experts, to review and assess the deployment of AI in national security contexts, ensuring regular audits and after-action reports are provided to relevant congressional committees.

At the same time, the federal judiciary must recognize the unique challenges posed by algorithmic opacity and actively adapt doctrines of reviewability and standing to ensure that technological complexity does not become a blanket shield for executive discretion. Courts should clarify that the invocation

284. *See* James E. Baker, *Practicing at the Speed of Relevance: Emerging Technologies and the Changing Nature of National Security Law, in* International Security Studies & Technology 76, 79–82 (Edward Elgar 2024) (explaining how AI and other emerging technologies impose novel legal and constitutional challenges in national security decision-making).

285. *See generally* Carol Harlow, *Transparency, Accountability and the Privileges of Power*, 22 Eur. L.J. 273, 276–80 (2016) (arguing that modern governance structures risk subordinating transparency and accountability to administrative or technical expedience).

286. *See* Bradley & Goldsmith, *supra* note 13.

287. *See* Coglianese & Lehr *supra* note 143.

288. *See generally* Erica H. Ma, *supra* note 153.

of the political question doctrine is not appropriate solely on the grounds of technological complexity or secrecy.[289] Judicial review should extend to the lawfulness of delegating critical national security decisions to autonomous systems, especially where such decisions have the potential to affect fundamental rights or implicate constitutional processes. Doctrinal tests for nondelegation and separation of powers should be updated to require a meaningful standard of human oversight and ethical deliberation when government relies on algorithmic decision-making in foreign affairs.

AI systems used in executive agreements, targeting, and surveillance must be subject to robust transparency and explainability requirements. The executive branch should be required to document and, where possible, publicly disclose the logic, training data, and decision parameters of algorithmic tools that influence foreign policy. Where full transparency is not feasible due to national security concerns, meaningful summaries and independent testing of algorithmic systems should be mandated, so that congressional committees, inspectors general, and, where appropriate, courts can assess the legality and risks of these technologies.

Legal reforms in the United States should be developed in dialogue with allied democracies and in consideration of emerging international norms. The United States should participate actively in multilateral forums aimed at developing principles for the responsible use of AI in security, diplomacy, and arms control. It should ensure that bilateral and multilateral agreements on AI-enabled systems include explicit provisions for transparency, accountability, and human oversight, thereby preventing the emergence of a "black box" arms race and promoting confidence.[290]

Legal frameworks should also emphasize the irreducible role of human judgment and expertise in foreign policy. Training and continuing education programs should be established for executive officials, congressional staff, and judges to enhance algorithmic literacy and ensure informed scrutiny of AI-driven policies. Statutes and executive orders should require that critical foreign policy decisions, especially those involving the use of force or significant international commitments, remain subject to the ultimate approval of a designated human authority. For instance, Executive Order 13960[291] promotes the use of trustworthy AI in the federal government.[292] It directs federal

289. *See generally* Rachel E. Barkow, *More Supreme Than Court? The Fall of the Political Question Doctrine and the Rise of Judicial Supremacy*, 102 Colum. L. Rev. 237, 244–52 (2002) (arguing that courts should not invoke the political question doctrine merely because an issue is complex or sensitive, reinforcing the need for judicial oversight in technologically challenging contexts).

290. *See, e.g.,* Anna Nadibaidze & Dov Greenbaum, *Governance of AI in the Military Domain: International Law, Norms, and Ways Forward*, *in* Oxford Intersections: AI in Society. 1, 4–7 (Oxford University Press, 2025) (arguing that the development of shared international principles for military AI is essential to reduce strategic instability and to ensure transparency, accountability, and legitimate state practice).

291. Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

292. Felicia Kalkman, *Lessons from Executive Order 13950: The Dangers of Regulating Government Contractors Through Executive Orders*, 51 Pub. Cont. L.J. 89, 120–23 (2021) (explaining how executive orders structure federal decision-making and impose procedural constraints, supporting the need for human authority over AI-enabled governmental actions).

agencies to adopt principles of transparency, accountability, and reliability in the use of AI, including in areas such as international relations and security.

The constitutional and democratic legitimacy of U.S. foreign policy will increasingly depend on whether law and institutions can adapt to the realities of algorithmic governance. The temptation to delegate complex or controversial choices to opaque technological systems is substantial, but the abdication of human responsibility and oversight is not a neutral or inevitable consequence of progress. Rather, it is a choice—one that can and must be bounded by robust legal norms and institutional checks. If left unchecked, the diffusion of AI into executive agreements and military operations risks not only rendering traditional mechanisms of oversight obsolete, but also displacing the core values of transparency, deliberation, and accountability that define constitutional democracy. The challenge of the algorithmic age is not to reject innovation, but to ensure that its adoption does not outpace or undermine the very structures designed to protect democratic governance. The future of U.S. foreign policy and its legitimacy in the eyes of the world depends on the willingness of Congress, the courts, and the legal academy to act decisively in defense of these foundational commitments.

In summary, this Article advocates for a paradigm shift: the law must move beyond a reactive posture and proactively establish the conditions under which AI can serve the public interest without compromising the constitutional framework of foreign relations. Only by embedding AI-enabled statecraft within an accountable, transparent, and human-centered legal framework can the United States fulfill both the promise of innovation and the demands of constitutional fidelity.