Washington Journal of Law, Technology & Arts

Volume 20 | Issue 1 Article 2

1-8-2025

THE COMPACT CLAUSE AND CYBERWAR

Josie Laing

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 20, ISSUE 1 — WINTER 2024

THE COMPACT CLAUSE AND CYBERWAR

Josie Laing[1]

ABSTRACT

This article seeks to bring attention to the potential modern utility of Article 1, Section 10, Clause 3: the Compact Clause.[2] This section of the Constitution has historically been archived. However, given cyberspace's ever-growing prominence, the Compact Clause should be reconsidered as cyber warfare presents a novel opportunity for states to exercise their sovereign rights.

Section 10 restricts states' powers to engage with foreign entities.[3] Without the consent of Congress, states cannot enter into agreements with foreign powers or engage in war.[4] These restrictions on states were necessary when the Constitution was drafted.[5] To navigate foreign affairs nimbly, the United States needed to act as a unified force. Given that individual states' interests can and will vary from national interests, there was a need for the states to be explicitly bound together. The internet has complicated this understanding of federalism. States are being hacked by foreign entities and the federal government is late to act. As a result, states are beginning to take matters into their own hands, disturbing the traditional balance of power between the states and the federal government.

This challenge of tradition prompts a review of history. States did not sacrifice their voices for free. In exchange for foreign influence, states were guaranteed protection by the federal military in the case of invasion or military threat.[6] States were promised that they need not fight stronger forces alone and were assured that the federal government would "wage defensive war" if a state was invaded.[7] Historically, the United States has honored this promise by developing itself as a military superpower.[8] As a country, the United States has prepared itself for threats arising from land, sea, or air.[9] However, cyberspace presents a new landscape in

---

[1] The author of this article attends the University of Washington School of Law and has a penchant for cyber neuroticism. Advisors Alex Alben and William Covington assisted in this article's construction. Under the cover of night and the glare of day, Jimmy Ostrowski provided necessary feedback.
[2] U.S. CONST. art. I, §10, cl. 3.
[3] *Id.*
[4] *Id.*
[5] STEPHEN MULLIGAN, CONG. RSCH. SERV., LSB10808, CONSTITUTIONAL LIMITS ON STATES' POWER OVER FOREIGN AFFAIRS (2004); Richard Epstein & Jack Rakove, *Article 1, Section 10*, NAT'L CONST. CTR.: INTERPRETATION & DEBATE (May 16, 2024), https://constitutioncenter.org/the-constitution/articles/article-i/clauses/767.
[6] *See* U.S. CONST. art. IV, § 4.
[7] Robert G. Natelson & Andrew T. Hyman, *The Constitution, Invasion, Immigration, and the War Power of States*, BRIT. J. AM. LEGAL STUDIES 13, (2004).
[8] Sinéad Baker & Thibault Spirlet, *The World's Most Powerful Militaries in 2023, Ranked*, BUS. INSIDER (Dec. 18, 2023), https://www.businessinsider.com/ranked-world-most-powerful-militaries-2023-firepower-us-china-russia-2023-5.
[9] *Our Forces,* U.S. DEP'T. OF DEF., https://www.defense.gov/about/our-forces/ (last visited May 16, 2024).

which the United States is not prepared, leaving room for states to advance their reserved war powers.[10]

This article examines whether states can defend themselves and their constituents against cyberattacks while remaining consistent with the spirit of the Constitution. Part 1 will examine the historical backdrop of Section 10 and provide an overview of the past and present interpretations of invasion, imminent danger, and other related concepts. Part II will argue that warfare is becoming less kinetic and increasingly digital. Such digitization has led to states being attacked by foreign adversaries and other actors without organized federal aid. Part III points out the constitutional leeway permitting states to act during this cyber-era. While Montana's attempt to ban TikTok, a popular social media platform, may not be constitutionally feasible, states may be able to take cyber matters into their own hands until the federal government can protect the United States in cyberspace.

[10] Glenn Gerstell, *I've Dealt with Foreign Cyberattacks. America Isn't Ready for What's Coming.*, N.Y. TIMES (Mar. 3, 2022), https://www.nytimes.com/2022/03/04/opinion/ive-dealt-with-foreign-cyberattacks-america-isnt-ready-for-whats-coming.html; James Coker, *Only 4% of the US States Fully Prepared for Cyber-Attacks Targeting Elections*, INFOSECURITY MAG. (Jan. 10, 2024) https://www.infosecurity-magazine.com/news/us-states-prepared-cyber-elections/.

TABLE OF CONTENTS

PART I

I. A BIT OF HISTORY

The Compact Clause details how states must defer to Congress "unless actually invaded, or in such imminent Danger as will not admit of delay."[11] While the world has experienced several revisions since 1788, this clause has remained untouched. Given the current lack of division of military powers between states and the federal government, this clause may seem undeserving of attention. This view, however, ignores the intentionality behind the clause's inclusion in the Constitution. James Madison described the creation of the Compact Clause to be "within reasonings which are either so obvious, or have been so fully developed, that they may be passed over without remark."[12] Yet what was obvious *then* may not be so obvious now. Although the existence of certain state powers may seem like a fever dream, it was once an unquestioned reality.

The Compact Clause diminished states' powers but did not abolish them. The preservation of state powers is no accident of semantics. Rather, the preservation reflects the history of the United States' unification. The States were familiar with the benefits of a "geostrategic vision" for a nation. The United Kingdom had demonstrated how military power could be amplified when countries unified.[13] The Founders determined that the success of the United States depended on a federally led approach to foreign affairs, prompting a consolidation of state power and the creation of a federal government.[14] However, this integration was not absolute. Just as the countries of the United Kingdom did not give up their sovereignty to form the United Kingdom, the states did not fully surrender their sovereignty to form a federal union.[15] The United States' geography demanded a geostrategic vision. The East Coast was vulnerable to potential threats from the sea and those surrounding the Union.[16] Threat of outside invasions were identified in early settlements by British colonizers.[17] Potential future attackers resulted in the establishment of the colony's right to self-defense.[18] In 1629, the Massachusetts

---

[11] U.S. CONST. art. I, §10, cl. 3.
[12] Thomas J. Cheeseman & James F. Blumstein, *State Empowerment and the Compact Clause*, 27 WM & MARY B. OF RTS. J., 775, 799 (2019).
[13] *Id.* at 785 ("As the Founders recognized, '[w]hen England, Wales, and Scotland were separate kingdoms, military competition between them invited invasion and foreign intrigue, triggering a heightened domestic militarization that threatened liberty. The indivisible union of England and Scotland at the outset of the eighteenth century gave island residents more room to breathe free.'" (quoting AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 45 (2005))).
[14] *Id.* at 784.
[15] Robert G. Natelson, *The Constitution and the False Doctrine of Inherent Sovereign Authority*, 24 FEDERALIST SOC'Y REV. 346 1, 2 (2023).
[16] Jason Mazzone, *The Security Constitution*, 53 UCLA L. REV. 29, 37 (2005) ("One threat was foreign invasion (including attacks from Indians). The proximity of British and Spanish was a constant source of unease.").
[17] Robert G. Natelson & Andrew T. Hyman, *The Constitution, Invasion, Immigration, and the War Power of States*, 13 BR. J. AM. LEG. STUD. 3, 11 (2004) ("AND WEE [i.e., the king] DOE further . . . give and graunte to the said Governor and Company, and their Successors, by theis Presents, that it shall and maie be lawfull . . . to incounter, expulse, repell, and resist by Force of Armes, as well by Sea as by Lande, and by all fitting Waies and Meanes whatsoever, all such Person and Persons, as shall at any Tyme hereafter, attempt or enterprise the Destruccon, Invasion, Detriment, or Annoyaunce to the said Plantation or Inhabitants . . .").
[18] *Id.*

Bay Colony was granted a royal charter permitting the colony to defend itself from invaders.[19] The rights to war powers were granted in this charter. As colonies became states, their rights as colonies were presumably sustained.

These powers are acknowledged by the expectations of states. The Articles of Confederation required states to maintain a state militia.[20] States were concerned that the Constitution would disband these rights, leading to the inclusion of the Compact Clause in the Constitution. The clause reportedly prevented Congress from fully usurping the states' military powers by backstopping a reserve of powers for states. John Marshall, a future Chief Justice of the Supreme Court, assured states that said powers would be protected in the Virginia Convention debates, stating "When invaded, [states] can engage in war; as also when in imminent danger. This clearly proves, that the States can use the militia when they find it necessary."[21] At the time of the Constitution's ratification, the federal government was still not firmly established, and states' militias were sustained by genuine necessity.[22] Threats from foreign powers remained post-ratification, resulting in a recognition of the states' preserved powers. In 1837, the Supreme Court identified the strength of a state's police powers, holding that New York could regulate vessels and thus engage with foreign entities.[23] The dissipation of state militias, however, did not innately terminate state rights—for a right does not deteriorate when unused.

What war, invasions, danger, and delay meant to the Framers was never specified and likely will never be stably defined. The meaning of these words is incredibly important to determine what can invoke the states' war powers. Section 10 declares that states cannot engage in "War" without the consent of Congress or without invoking their war powers. The Department of Defense notes that "the precise definition of 'war' often depends on the specific legal context in which it is used."[24] Case law has interpreted "invasion" to mean a hostile entry by a foreign army.[25] The Compact Clause grants state powers if "actually invaded," while the Invasion Clause requires federal protection from "invasion."[26] Thus, the Invasion Clause allows for the federal government to act preemptively while the Compact Clause relies on an event having occurred.[27] This article focuses on what this exception clause could mean for states when applied to

---

[19] *Id.*
[20] *Id.* at 13.
[21] *Id.* at 16-17 (discussing ratification debates in Virginia).
[22] Gregory Ablavsky, *Stanford's Greg Ablavsky on Law and the History of American Militias*, STAN. L. SCH. BLOGS (Oct. 12, 2020), https://law.stanford.edu/2020/10/12/stanfords-greg-ablavsky-on-law-and-the-history-of-american-militias/.
[23] The Mayor, Aldermen and Commonalty of New York v. George Miln, 36 U.S. 102, 132-33 (1837) ("The power then of New York to pass this law having undeniably existed at the formation of the constitution, the simple inquiry is, whether by that instrument it was taken from the states, and granted to congress; for if it were not, it yet remains with them. If, as we think, it be a regulation, not of commerce, but police; then it is not taken from the states.").
[24] DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 16 (2023), https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF [hereinafter DOD MANUAL].
[25] Robert G. Natelson & Andrew T. Hyman, *The Constitution, Invasion, Immigration, and the War Power of States*, 13 BR. J. AM. LEG. STUD. 3, 11 (2004) (citing California v. United States, 104 F.3d 1086, 1091 (9th Cir. 1997)); Padavan v. United States, 83 F.3d 23, 28 (2d Cir. 1996); New Jersey v. United States, 91 F.3d 463, 468 (3d Cir. 1996) (all interpreting "invasion" as limited to an incursion by a foreign army).
[26] U.S. CONST. art. IV, § 4.
[27] *Id.*

cyberspace.[28] Cyberwarfare is rapidly emerging as the battleground of the future, with state governments experiencing cyberattacks with frightening regularity. [29] The federal government is attempting to ramp up its cyber defense efforts but remains incapable of providing a strong defense for the country.[30] Consequently, while Section 10's Exception Clause may implicate traditional notions of the Constitution's division of war powers, state sovereignty cannot be ignored. Thus, while states' need for defenses dissipated over the years, the Exception Clause remains untouched and thus constitutionally empowered.[31] This article intends to examine whether states are constitutionally permitted to act in response to cyber-attacks or threats.

PART II

I. QUICK, COVER! STATES ARE UNDER ATTACK!

The laws we know today, both domestic and international, were developed in a world tied to land, sea, and air. Cyberspace presents a challenge to these developed legal systems, for its existence hovers somewhere between the corporeal and the immaterial. Despite its abstract presence, cyberspace creates opportunities for real harm. Cyberwarfare threatens both the safety of individuals and the stability of cyberspace's infrastructure. States have an interest in protecting their citizens and thus have an interest in preventing cyber harm. Accordingly, states have an obligation to understand the dangers of cyberspace and defend their constituents from such digital invasions.

Cyberspace can facilitate many types of harm.[32] The internet presents opportunities for cybercrimes including, but not limited to, the distribution of malware or DDoS attacks.[33] Federal and state infrastructure is particularly susceptible to these attacks.[34] An example of the scale of the danger involves the U.S. electrical grid, which millions of Americans rely on for their

---

[28] *Cyber Attack*, NAT'L INST. OF STANDARDS & TECH.: GLOSSARY, https://csrc.nist.gov/glossary/term/cyber_attack#:~:text=An%20attack%2C%20via%20cyberspace%2C%20targeting,NIST%20SP%20800%2D30%20Rev ("Cyberspace may be defined as "[a] global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.") (Multiple definitions of cyber attack are provided including "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.").

[29] *Id.* ("The term 'attack' often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services."); Julie Pattison-Gordon, *Justice Hacked: When Cyber Criminals Come for the Courts*, GOV'T TECH. (Dec. 7, 2022), https://www.govtech.com/security/justice-hacked-when-cyber-criminals-come-for-the-courts.

[30] Gordon Chang, *Terrifying Hacks on Critical Infrastructure Have Arrived. America Isn't Ready.*, THE HILL (Dec. 12, 2023), https://thehill.com/opinion/cybersecurity/4353922-terrifying-hacks-on-critical-infrastructure-have-arrived-america-isnt-ready/.

[31] U.S. CONST. art. III, § 2, cl 2.

[32] Ben Woods, *Viruses, Trojans, Malware, Worms – What's the Difference?*, WIRED (May 9, 2017), https://www.wired.com/story/ransomware-viruses-trojans-worms/.

[33] *Id.*

[34] Nathaniel Herz, *Hackers Have Penetrated Multiple Alaska Agencies This Year. Here's What We Know.*, ALASKA PUB. MEDIA (June 23, 2021), https://alaskapublic.org/2021/06/23/qa-hackers-have-penetrated-multiple-alaska-agencies-this-year-heres-what-we-know/.

electricity. The system is vulnerable to cyberattacks because the infrastructure has been necessarily digitized. In 2009, such critical infrastructure was reportedly hacked by foreign adversaries.[35] This attack did not disrupt energy access for Americans, but it did establish that the U.S. needs some bulwarks.

In 2021, Americans experienced a resource interruption.[36] For five days, the Colonial Pipeline's operations came to a halt because hackers boarded their servers and demanded ransom.[37] The attack caused a price surge amid fears of gas shortages, as Colonial Pipeline is the dominant fuel supplier to the East Coast.[38] Such attacks on private infrastructure may prompt more government involvement in private companies' security practices. However, the U.S. government has its own street to clean up, as critical governmental infrastructure is compromised by state-sponsored actors.[39]

These attacks reflect the modern weaknesses of the United States. Private, state, and federal infrastructure directly dictate the security of people's lives. When that infrastructure is threatened, so is the safety of Americans. While cyberattacks can inflict severe economic costs, it is worth noting that the risks also extend to life and limb.[40] Intrusions into critical infrastructure are not one-offs, rather they represent the future of foreign adversary acts of espionage and aggression. State infrastructure is potentially more vulnerable than federal infrastructure. State court systems have been infiltrated and transportation services ambushed, but despite tangible threats, most states operate with limited cyber budgets.[41] While there has been a wave of federal

---

[35] Chuck Brooks, *3 Alarming Threats to The U.S. Energy Grid – Cyber, Physical, And Existential Events*, FORBES (Feb. 15, 2023), https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/?sh=114d4942101a; Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, WALL ST. J. (Apr. 8, 2009), https://www.wsj.com/articles/SB123914805204099085#printMode.

[36] Kimberly Wood, *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack*, GEO. ENV'TL L. REV. (Mar. 7, 2023), https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/.

[37] *Id.*

[38] *See id.*

[39] *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 7, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[40] *On-the-Record Press Call on the Biden-Harris Administration Initiative to Bolster the Cybersecurity of U.S. Ports*, THE WHITE HOUSE (Feb. 20, 2024), https://www.whitehouse.gov/briefing-room/press-briefings/2024/02/21/on-the-record-press-call-on-the-biden-harris-administration-initiative-to-bolster-the-cybersecurity-of-u-s-ports/; Aarian Marshall & Will Knight, *The White House Warns Cars Made in China Could Unleash Chaos on US Highways*, WIRED (Feb. 29, 2024), https://www.wired.com/story/china-cars-national-security-threat-investigation/ (discussing Chinese cars crashing on freeways); *Harnessing Water, Defending Data: Cybersecurity in Hydropower and Dam Facilities*, GROUND CONTROL (Sept. 18, 2023), https://www.groundcontrol.com/blog/harnessing-water-defending-data-ensuring-cybersecurity-in-hydropower-and-dam-facilities/; Susan Pickering & Peter Davis, *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, GEO. J. INT'L AFF.: SCI. & TECH. (Jan. 22, 2021), https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/ (other examples of critical infrastructure vulnerable to attacks include dams and nuclear power plants).

[41] Nathaniel Herz, *Hackers have Penetrated Multiple Alaska Agencies This Year. Here's What We Know.*, ALASKA PUB. MEDIA (June 23, 2021), https://alaskapublic.org/2021/06/23/qa-hackers-have-penetrated-multiple-alaska-agencies-this-year-heres-what-we-know/; Laurel Demkovich, *Cyberattack Crashes Parts of WA Transportation Website*, WASH. STATE STANDARD (Nov. 9, 2023), https://washingtonstatestandard.com/2023/11/09/cyberattack-crashes-wa-transportation websites/#:~:text=A%20major%20cyberattack%20hit%20the,employees%20for%20private%20construction%20contractors; Megan Reiss, *States Are the Weak Links on Cyber Security*, R ST. (Jan. 24, 2019),

grants to fund state, local, and tribal cyber efforts, there is a tremendous need for more resources.[42] The internet creates the perfect conditions for asymmetrical warfare, in which individuals can attack and inflict serious damage on large organizations or governments, necessitating the implementation of defenses from both small and large entities.[43] Often, these smaller attackers are sponsored by large entities. State-sponsored attackers are at the center of cyberwarfare and provoke legally complicated questions about anonymous attacks, so-called "flagless" attacks.

II. THE TRICKINESS OF STATE-SPONSORED ATTACKERS

Foreign adversaries sponsor cyber-attacks, presenting a challenge to the cybersecurity of the federal government and state governments. Six countries are listed as U.S. foreign adversaries: China, Cuba, Iran, North Korea, Russia, and the regime of Venezuelan politician Nicolas Maduro.[44] To make the list, the Secretary of State must determine that "foreign governments or foreign non-government persons have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."[45] China, Iran, North Korea, and Russia have the strongest potential to inflict harm on the United States through cyberspace.[46] While it can be difficult to directly link foreign adversaries with a cyber-attack, state-sponsored hacking groups are on the rise. The danger of cyber hacks is not limited to stolen data. Hacking can also allow for data to be manipulated, deleted, or secretly surveilled—placing critical infrastructure at risk.[47]

China has been singled out as a technological competitor and security threat in recent years. In 2020, FBI Director Christopher Wray commented on a security breach saying, "If you are an American adult, it is more likely than not that China has stolen your personal data."[48] In 2024, Wray divulged that "China's hacking teams outnumber FBI's cyber agents 50 to 1."[49] To note, this comparison leaves out other government forces that engage in cyberoperations such as

---

https://www.rstreet.org/commentary/states-are-the-weak-links-on-cyber-security/; Jenni Bergal, *State Cybersecurity Offices Need More Money and Staff, Report Finds*, STATELINE: PART OF STATES NEWSROOM (Oct. 23, 2018), https://stateline.org/2018/10/23/state-cybersecurity-offices-need-more-money-and-staff-report-finds/.

[42] Colin Wood, *Local Governments Don't Have Enough Cyber Funding, Survey Finds*, STATESCOOP (Nov. 15, 2023), https://statescoop.com/pti-cybersecurity-survey-local-government/.

[43] John Dever & James Dever, *Cyberwarfare: Attribution, Preemption, and National Self Defense*, 1 J.L. & CYBER WARFARE 26 (2013).

[44] Determination of Foreign Adversaries, 15 C.F.R. § 7.4 (2024).

[45] *Id.*

[46] HCI FOR CYBERSECURITY, PRIVACY AND TRUST, (Abbas Moallem ed., 1st ed. 2023); American Cyber Defense Agency, *Nation-State Cyber Actors*, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (last visited Nov. 20th, 2024).

[47] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[48] Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States, Remarks at the Hudson Institute Video Event: China's Attempt to Influence U.S. Institutions*, FBI NEWS (July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states (last visited Oct. 23, 2024).

[49] Sean Lyngass, *Suspected Chinese Hackers Target US Research Organization in Latest Spying Spree*, CNN: POLITICS (Jan. 10, 2024), https://www.cnn.com/2024/01/10/politics/chinese-hackers-research-organization/index.html.

the Cyber Command and the NSA.[50] Concerns about China also extend to Chinese companies, as the Chinese government is believed to have access to data held by these companies.[51] The economic and military tensions between the United States and China are steadily escalating. Taiwan is an example of crossfire, for despite China's efforts to envelop Taiwan, the country remains independent. This independence relies on the United States' support. Taiwan produces world-class semiconductor chips—chips that China can't seem to build itself. [52] This production ability makes Taiwan a critical player in the global race to improve technology. It also makes Taiwan a focal point for China's goals, as these chips will dictate the future of artificial intelligence and modern warfare.[53] Malicious code was recently discovered within U.S. military networks, suspected to have been implanted by China.[54] The code was installed in networks that control power grids, water supplies, and communication systems and, if activated, could have devastating impacts on the US military and ordinary American citizens. Officials suspect that the code was preemptively implanted in advance of a dispute between Beijing and the United States over Taiwan.[55]

Cyberattacks serve multiple functions. They can be preemptive, laying the foundation for future action. They can also be intertwined with kinetic warfare. A future invasion of Taiwan would occur on land and potentially through cyberspace. The United States has identified China as the "broadest, most active, and persistent cyber espionage threat to the U.S. government and private-sector networks."[56] China has shown the capability to conduct attacks that could severely impact the U.S. military's operations and disable critical domestic infrastructure. The U.S. has also identified China's cyber threat to include efforts to silence critiques of the Chinese Communist Party, including attacks that occur beyond the U.S. territorial boundaries.[57]

Russia has also been identified as one of the most prominent cyber threats to the U.S.[58] In 2020, a Texas-based company called SolarWinds was allegedly attacked by Russia-sponsored hackers.[59] SolarWinds, an information technology company used for IT resources, was

---

[50] Interview with Jimmy Ostrowski, J.D. Candidate, University of Washington School of Law, in Seattle, Wash. (Dec. 7, 2023).

[51] Zhizheng Wang, *Systematic Government Access to Private-Sector Data in China*, 2 INT'L DATA PRIV. L. 220, 229 (2012).

[52] Chris Miller, *The Chips That Make Taiwan the Center of the World*, TIME (Oct. 5, 2022, 6:00 AM), https://time.com/6219318/tsmc-taiwan-the-center-of-the-world/.

[53] Rob Toews, *The Geopolitics of AI Chips Will Define the Future of AI*, FORBES (May 7, 2023, 7:00 PM), https://www.forbes.com/sites/robtoews/2023/05/07/the-geopolitics-of-ai-chips-will-define-the-future-of-ai/?sh=4ae590ac5c5c.

[54] David Sanger & Julian Barnes, *U.S. Hunts Chinese Malware That Could Disrupt American Military Operations*, N.Y. TIMES (July 29, 2023), https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

[55] *Id.*

[56] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[57] *Id.*

[58] *Russia Cyber Threat Overview and Adversaries*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia (last visited Nov. 3, 2024).

[59] Isabella Jibilian & Katie Canales, *The US Is Readying Sanctions Against Russia Over the SolarWinds Cyberattack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal,* BUS. INSIDER (Apr. 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12; Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

compromised when malicious code was introduced into a software update, which then infiltrated companies and government agencies alike.[60] One of the affected government agencies was the Cybersecurity and Infrastructure Agency.[61] Despite the United States' unwavering accusations, Russia denies involvement. The attack was deemed "too novel" to be detected by current detection software, raising alarm as to how secure cyber defenses really are in the face of constant innovation.[62] The potential of these attacks is frightening. Russia's recent military action against Ukraine demonstrates a capacity for unprovoked aggression.[63] Russia has utilized its cyber operations to both destroy and discredit Ukraine's government. The strategy for these attacks was evident on February 24, 2022, hours before Russia invaded Ukraine. A cyberattack was allegedly conducted by the same Russian military intelligence agency and disabled satellites that involved command of Ukrainian troops. This Russian intelligence agency was the same one that hacked the Democratic National Committee in 2016, leading to the WikiLeaks email leak.[64]

The United States has also publicly accused North Korea of conducting cyberattacks.[65] In 2014, Sony experienced a tremendously devastating hack that paralyzed the company's operations and resulted in millions in damages. It is worth noting that a description of the attack details how the cyberattack artificially incorporated typical war-like characteristics: "Employees logging on to its network were met with the sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives."[66] Attacks like this affect both the United States economy and stance in geopolitics. When a country has been identified to be behind a hack, the United States has an obligation to respond.[67] The United States cannot turn a blind eye to countries that actively aim to harm U.S. companies. Whether this response involves a returned cyberattack, sanctions, or other measures, cyberspace is not immune from a severe governmental response.

PART III

I. FEDERAL RESPONSE (OR LACK THEREOF)

The federal government is struggling to prepare for the future of the United States in cyberspace. Congress and the White House have taken steps to restructure and develop cyber

---

[60] Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[61] *Id.*
[62] *Id.*
[63] David Sanger & Kate Conger, *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds*, N.Y. TIMES (May 10, 2022), https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html#:~:text=The%20attack%20was%20focused%20on,wiper%E2%80%9D%20software%20that%20destroys%20data.
[64] Mark Hosenball & David Alexander, *Democrats Sue Russia, Trump Campaign for Alleged 2016 Election Conspiracy*, REUTERS (Apr. 20, 2018), https://www.reuters.com/article/idUSKBN1HR2BE/.
[65] David Sanger & Nicole Perlroth, *U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.
[66] Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 990 (2018).
[67] DOD MANUAL, *supra* note 24 ("As a matter of national policy, the United States has expressed the view that when warranted, it will respond to hostile acts in cyberspace as it would to any other threat to the country.").

defenses, but these steps are scattered across the federal plain. Several different federal agencies take on cybersecurity efforts including the National Institute for Standards and Technology (NIST), the Cybersecurity Infrastructure Security Agency (CISA), the U.S. Cyber Command (a military operation), and the National Cyber Director's Office stationed at the Whitehouse.[68] The Federal Trade Commission handles privacy issues, as privacy protections have historically found legal standing in consumer protections given the lack of explicit federal or state private laws.[69] These agencies are facing a wide swath of complicated security problems and are trying to bail out what water they can.[70] Yet the structure and the youth of these federal agencies reveal a juvenile defense force. For instance, CISA is a relatively recent creation, established in 2018.[71] Federal acknowledgment of cybersecurity demands are reflected in CISA's consistently expanding budget.[72] Yet, despite efforts to construct a robust cybersecurity center, CISA was attacked in 2024.[73] This attack signals how cyberspace orchestrates an environment in which the United States is under perpetual attack.[74] The official Cybersecurity Strategy of 2024 emphasizes protecting data and establishing defenses from cyberattacks.[75] The cost of supporting these efforts is often incalculable but definitively sizable.[76] Given the novelty of the problem and bureaucratic challenges, the federal government is unprepared for cyberattacks, which continue to rise. Cyberattacks will not wait for the federal government to regroup, a reality that has resulted in legislative vigor in federal and state governments.[77] An example of this legislative response is the saga of TikTok and WeChat legislation.

II. TIKTOK AND WECHAT

In recent years, the federal government has legislatively targeted private companies with foreign origins. In 2020, President Trump issued two executive orders to ban TikTok and WeChat, apps that facilitate social media and communication.[78] However, these orders were not

---

[68] Scott Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86 (2023).
[69] *Id.*
[70] Christian Vasquez, *CISA Faces Resource Challenge In Implementing Cyber Reporting Rules*, CYBERSCOOP (Apr. 2, 2024), https://cyberscoop.com/cisa-circia-cyber-incident-reporting/.
[71] Chris Riotta, *CISA Turns Five and Looks to the Future*, NEXTGOV FCW (Nov. 16, 2023), https://www.nextgov.com/cybersecurity/2023/11/cisa-turns-5-and-looks-future/392080/.
[72] *Id.*
[73] Jonathan Reed, *CISA Hit by Hackers, Key Systems Taken Offline*, SEC. INTEL. (Mar. 18, 2024), https://securityintelligence.com/news/cisa-hackers-key-systems-offline/.
[74] *Id.*
[75] *The U.S. Now Has a National Cybersecurity Strategy, but Is It as Strong as It Could Be?*, U.S. GOV'T ACCOUNTABILITY OFF. (Mar. 21, 2024), https://www.gao.gov/blog/u.s.-now-has-national-cybersecurity-strategy-it-strong-it-could-be.
[76] *Id.*
[77] Maggie Miller & Lara Seligman, *The U.S. Is Getting Hacked. So the Pentagon Is Overhauling Its Approach to Cyber*, POLITICO (Sept. 9, 2023), https://www.politico.com/news/2023/09/12/pentagon-cyber-command-private-companies-00115206.
[78] Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 48, 637 (Aug. 6, 2020) [hereinafter TikTok Order]; Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 48, 641 (Aug. 6, 2020) [hereinafter WeChat Order].

sustained when challenged.[79] Nevertheless, the orders demonstrated the federal government's interest in limiting foreign company access to the data of Americans.

The WeChat case was significant for several reasons. First, it highlighted growing concerns about China's rise in cyber power. Additionally, the case partially supported the legitimacy of these concerns. The WeChat case arose in 2020 on the premise that transactions related to WeChat were a risk to national security.[80] The White House issued an executive order prohibiting such transactions, stating that WeChat's presence in the United States presented an "undue risk of sabotage or subversion" to domestic communication technologies. The order was contested and the court ultimately found that WeChat was entitled to an injunction because WeChat facilitated personal communications, making the ban an abuse of authority.[81] Nonetheless, the court acknowledged that China posed a national security threat. Despite this, the court determined that the evidence presented about the severity of the security threat was insufficient to overcome the order's constitutional issues.[82] The WeChat case demonstrated that the federal government is willing to perceive data collection by foreign private companies as a sufficient threat to invoke national security concerns. The first efforts at a federal TikTok ban echoed these sentiments, cementing a national position on the threat of data collection and the geopolitical complications of cyberspace. [83]

In 2020, TikTok was named in another executive order. Since its launch in 2016, the social media company emerged as the poster child for China's cloak-and-dagger efforts to undermine the United States.[84] On account of its data collection and supposed algorithmic manipulation, TikTok has been characterized as a wolf in electric sheep's clothing.[85] Fears that the Chinese government is controlling this private Chinese company resulted in a Congressional hearing on March 23, 2023.[86] While TikTok's CEO attempted to assure lawmakers that the Chinese government could not manipulate the app, many remained unconvinced.[87] A powerful example in support of these fears included the Justice Department's investigation into TikTok's leak of an

---

[79] Bobby Allyn, *U.S. Judge Halts Trump's TikTok Ban, The 2nd Court to Fully Block the Action,* NPR (Dec. 7, 2020), https://www.npr.org/2020/12/07/944039053/u-s-judge-halts-trumps-tiktok-ban-the-2nd-court-to-fully-block-the-action; Bobby Allyn, *Federal Judge Blocks Trump Administration's U.S. WeChat Ban,* NPR (Sept. 20, 2020), https://www.npr.org/2020/09/20/914983610/federal-judge-blocks-trump-administrations-u-s-wechat-ban.

[80] WeChat Order, *supra* note 78.

[81] U.S. WeChat Users Alliance v. Trump, 488 F. Supp. 3d 912, 926 (N.D. Cal. 2020).

[82] *Id*. ("Finally, the government cited reports identifying Tencent and WeChat as a growing threat and citing an Australian nonpartisan think tank's report (1) discussing the Chinese government's "highly strategic foreign policy" to become "the strongest voice in cyberspace" . . . While the general evidence about the threat to national security related to China (regarding technology and mobile technology) is considerable, the specific evidence about WeChat is modest.").

[83] Sara Morrison, *Maybe Trump Was Right about TikTok*, VOX (Dec. 13, 2022), https://www.vox.com/recode/23453786/tiktok-bytedance-cfius-data-trump-ban.

[84] Associated Press, *How TikTok Grew From a Fun App for Teens Into a Potential National Security Threat*, SECURITYWEEK (Apr. 29, 2024), https://www.securityweek.com/how-tiktok-grew-from-a-fun-app-for-teens-into-a-potential-national-security-threat/.

[85] *Id.*

[86] Dara Kerr, *Lawmakers Grilled TikTok CEO Chew for 5 Hours in a High Stakes Hearing about the App*, NPR (Mar. 23, 2023), https://www.npr.org/2023/03/23/1165579717/tiktok-congress-hearing-shou-zi-chew-project-texas.

[87] Yaqiu Wang, *The Problem with TikTok's Claim of Independence from Beijing*, HUM. RTS. WATCH (Mar. 24, 2023), https://www.hrw.org/news/2023/03/24/problem-tiktoks-claim-independence-beijing.

American journalist's data.[88] While the orders were halted by the judicial branch and the Biden administration eventually dropped them, efforts to address concerns about foreign adversaries continued. Senator Marco Rubio introduced a bill that directly addressed social media companies headquartered in foreign adversary countries.[89] Notably, the bill applied to companies that are subject to indirect as well as direct influence by suspect countries.[90] TikTok efforts came to a head in the Spring of 2024 when Congress passed a law requiring TikTok to sell to a government-approved buyer or otherwise, face a ban from the U.S. market.[91] A complete elimination of the app would likely not be well received by the public because many Americans depend on WeChat and TikTok for communication, resources, and income. Furthermore, First Amendment concerns that speech was being stifled were pulled to the forefront, echoing those in the WeChat case.[92] However, widespread fear of foreign espionage and subversive political destabilization continue to carry the national security torch forward into cyberspace.

Most strikingly, states have taken their hand at carrying this torch. In 2023, Montana passed a law banning TikTok, raising eyebrows for several reasons.[93] One of these reasons is found in the first line of the Act.[94] The line reads "WHEREAS, the People's Republic of China is an adversary of the United States and Montana."[95] While Montana is correct to list China as a foreign adversary of the United States, one might question whether China is an enemy of Montana.[96] Montana's decision to include itself as a separate entity in addition to the United States represents a perceived truth about the nature of foreign cyber threats. China can cause damage to both the United States as a whole and to states individually. Accordingly, China is an enemy of two governments. While states are typically restricted from involving themselves in foreign affairs, the law demonstrated Montana's intention to position the state as a player in foreign cyber affairs. Montana's position that TikTok needed to be banned was confirmed by Congress in 2024.[97] The state's insistence on getting involved however, reflects a new challenge to the status quo of traditional federalism.

When Montana attempted to ban TikTok, the social media company immediately challenged the law and requested an injunction.[98] TikTok's brief highlighted Montana's dissatisfaction with the state of federal cyber protection and described the legislature's discontent with federal inaction in regulating foreign technology.[99] TikTok recited expressions of discontent by bringing attention to statements made by Montana's Attorney General and Senator Shelley

---

[88] Glenn Thrush & Sapna Maheshwari, *Justice Dept. Investigating TikTok's Owner Over Possible Spying on Journalists*, N.Y. TIMES (Mar. 17, 2023), https://www.nytimes.com/2023/03/17/us/politics/tik-tok-spying-justice-dept.html.

[89] Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party Act, S.347, 117th Cong. (2023).

[90] *Id.*

[91] Sapna Maheshwari & Amanda Holpuch, *Why the U.S. Is Forcing TikTok to Be Sold or Banned*, N.Y. TIMES (May 8, 2024), https://www.nytimes.com/article/tiktok-ban.html.

[92] Vittoria Elliott & Makena Kelly, *Can the First Amendment Save TikTok?*, WIRED (Apr. 24, 2024), https://www.wired.com/story/tiktok-ban-first-amendment-courts-challenge/.

[93] An Act Banning TikTok in Montana, S.B. 419, 68th Leg., Reg. Sess., Preamble (Mont. 2023), https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf [hereinafter S.B. 419].

[94] S.B. 419.

[95] *Id.*

[96] Determination of Foreign Adversaries, 15 C.F.R. § 7.4 (2024).

[97] Sapna Maheshwari & David McCabe, *Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part*, N.Y. TIMES (Apr. 23, 2023), .

[98] Alario v. Knudsen, 704 F. Supp. 3d 1061 (D. Mont. 2023).

[99] *Id.*

Vance.[100] The Attorney General reportedly said that "there's no guarantee that the feds are actually going to act here."[101] When describing the purpose of the Act, Senator Vance declared "[the purpose is] to send a message to other states and to Congress" because she has "no faith in our national administration."[102] Whether the Act was intended to successfully dismantle TikTok's operations in Montana or to proactively send a message, news coverage made it clear that Montana was acting out of character.[103]

The unusual law sparked attention in the judicial system, leading to TikTok being granted an injunction.[104] The judge found that "Montana does not have an important government interest in regulating foreign affairs."[105] While TikTok is typically banned on state and federal devices on the basis of security concerns, it is rare to ban social media or communications technology for civilians because of foreign affair concerns.[106.] In fact, as the judge held, it is improper for a state to meddle with civilian's lives on such grounds. The court's decision anchored itself in constitutional precedent and impact, noting that even if the bill was directed at restricting foreign access to Montanans, the bill lacked efficacy because of the mechanics of data collection.[107] The court described how foreign adversaries could collect data through data brokers, open source gathering, and hacking.[108] However, this hiccup did not stop Montana from legislating in the foreign affairs arena. Montana's legislature recently passed a bill that regulates genetic data and restricts Montanans' data from being "stored within the territorial boundaries of any country sanctioned in any way by the United States office of foreign asset control or designed as a foreign adversary."[109] This condition is more subtle than the TikTok ban but still impacts foreign matters. The law, however, is wrought with enforcement challenges because if the regulated data *is* stored within a foreign adversary's territorial boundaries, who will protect it?

PART IV

I. STATES ENTER THE FRAY!

The Compact Clause is a self-defense clause. After ratification, states' war powers were collapsed, compressed, and stored away in a paragraph. These powers have remained dormant in storage since 1788, but cyberspace presents an opportunity for a revival.[110] Current understandings of federalism indicate that states do not have foreign affairs powers. When

---

[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] SANCHITHA JAYARAM ET AL., CONG. RSCH. SERV., LSB10972, MONTANA'S TIKTOK BAN, AN INJUNCTION, AND PENDING LEGAL ACTIONS (2023).
[104] Alario v. Knudsen, 704 F. Supp. 3d 1061 (D. Mont. 2023).
[105] *Id.*
[106] *TikTok Banned on U.S. Government Devices, and the U.S. Is Not Alone. Here's Where The App Is Restricted*., CBS NEWS (Mar. 1, 2023), https://www.cbsnews.com/news/tiktok-banned-us-government-where-else-around-the-world/.
[107] *Id.*
[108] *Id.*
[109] Genetic Information Privacy Act, S. 419, 68th Leg., Reg. Sess., Preamble (Mont. 2023), https://leg.mt.gov/bills/2023/billpdf/SB0351.pdf.
[110] *See generally The Day the Constitution Was Ratified*, NAT'L CONST. CTR. (June 21, 2023), https://constitutioncenter.org/blog/the-day-the-constitution-was-ratified.

geopolitical tensions rise, the federal government reigns supreme. This narrow conception of the states' powers is partly due to a historic lack of need for Section 10, as the federal government established a military presence that has protected states from dangers. Cyberspace distorts this precedent. Accordingly, the traditional balance of state and federal powers may need an update. When the federal government fails to protect states from cyber harms, states may have cause to invoke their Constitutional rights. States have a duty to protect their infrastructure and residents, and federal inaction on the cyber front can jeopardize state property and people, potentially reviving State self-defense powers.

The Supreme Court has taken the stance that foreign affairs are exclusively federal issues.[111] States, however, are routinely involved in foreign matters.[112] The Internet has blurred the boundaries of foreign involvement between the states and the federal government. For instance, states cannot successfully legislate cyber matters without reaching beyond their borders. State laws regarding data regulation are focused on protecting state residents. [113] Since data is not always stored in servers in the United States, much less in the state, these state laws address issues beyond their scope. State legislation in cyberspace can have widespread effects through minority rule. This impact is exemplified through data laws. The state that sets the strictest laws on data collection often sets the standard for the country because businesses don't want to waste energy ensuring state-by-state compliance.[114] While critics of this system call for federal action, federal presumption is years away.[115] Cyberspace has thus required states to participate in legislation involving foreign affairs with national effects.

The potential for state action to have a nationwide impact is significant. As Congress is slow to answer calls, state interest in state action is on the rise.[116] As a result, the backwater clause of Section 10 has garnered interest. Recent intrigue has emerged in the immigration context, suggesting the clause's modern relevancy. Texas has interpreted the meaning of invasion in Section 10 to apply to immigration.[117] Texas Governor, Greg Abbott, claimed that the federal government has a Constitutional obligation to protect states against invasions and

---

[111] STEPHEN MULLIGAN, CONG. RSCH. SERV., LSB10808, CONSTITUTIONAL LIMITS ON STATES' POWER OVER FOREIGN AFFAIRS (2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10808.

[112] *Id.*; Press Release, *DiNapoli Orders Divestment of Russia Holdings*, OFF. N.Y. STATE COMPTROLLER (Mar. 25, 2022) ("New York State Comptroller Thomas P. DiNapoli, sole trustee of the New York State Common Retirement Fund (Fund), today announced that he has directed divestment from Russian companies and continued his prohibition of any further investments in them.").

[113] *See United States Data Breach Notification in the United States 2023 Report*, PRIV. RTS. CLEARINGHOUSE (Oct. 5, 2023), https://privacyrights.org/resources/united-states-data-breach-notification-united-states-2023-report; David Navetta, Michael Egan, Lei Shen, Gary Hunt III, Allison Kutner, *California's Delete Act – Key Takeaways for Data Brokers*, COOLEY (Oct. 16, 2023), https://cdp.cooley.com/californias-delete-act-key-takeaways-for-data-brokers/.

[114] Natasha Singer, *Charting the 'California Effect' on Tech Regulation* N.Y. TIMES (Oct. 12, 2022), https://www.nytimes.com/2022/10/12/us/california-tech-regulation.html ("Given California's clout as the most populous state with the largest economy, many online services may simply make changes nationwide to comply with the new rules, rather than treat consumers in California differently.").

[115] Catherine Stupp, Patchwork of State Privacy Laws Remain After Latest Failed Bid for Federal Law, W.S.J. (Aug. 27, 2024), https://www.wsj.com/articles/patchwork-of-state-privacy-laws-remains-after-latest-failed-bid-for-federal-law-2a1a020d.

[116] Coraleine Kitt, *The Shifting Landscape of U.S. State Data Privacy Laws in 2024*, THE LEGAL INTEL. (Sept. 17, 2024), https://www.law.com/thelegalintelligencer/2024/09/17/the-shifting-landscape-of-us-state-data-privacy-laws-in-2024/?slreturn=2024121621329.

[117] Alex Nowrasteh, *Explaining the Border Standoff Between Texas and the Federal Government*, CATO INST. (Jan. 27, 2024), https://www.cato.org/blog/explaining-border-standoff-between-texas-federal-government.

when these duties are abandoned, states have the right to self-defense.[118] While there is some scholarly support for tying the meaning of invasion to immigration, it is legally suspect as case law and historical sources do not always support such a denotation.[119] Notably, a court decision on the "immigration is invasion" issue cited the Civil War as the end of state rights which hamstring federal authority.[120] Were state war powers annexed by the federal government after the Civil War? While the use of Section 10 in the immigration context may be a fool's errand, the semantics of "invasion" and "imminent danger" in cyberspace are still under review.

Exploration into the applied meaning of "invasion" and "imminent danger" is critical as the law hinges on clear definitions. Such zeal for definitions can lead to limited remedies. If a person experiences a unique harm, they may be left without a course of action if the wrong does not fulfill the defined meaning of a legal term. Clear terminology is often helpful, allowing for reliance to blossom. However, when considering the meanings of Section 10's words, it is important to recognize that ambiguity was threaded into almost every foundational legal text in this country. The Constitution was written without footnotes and thus the Compact Clause must be read without detailed instruction. The clause establishes two ways in which an attack could catalyze state-lead self-defense: when a state is "actually invaded" and when a state is "in such imminent Danger as will not admit of a delay."[121] The clause does not use language about "acts of war."[122] Rather, the language is more generous, allowing the Section to be invoked in a

---

[118] *Id.* (Governor Greg Abbott commenting on Compact Clause: "I have already declared an invasion under Article I, § 10, Clause 3 to invoke Texas's constitutional authority to defend and protect itself. That authority is the supreme law of the land and supersedes any federal statutes to the contrary."); Steve Vladeck, *Governor Abbott's Perilous Effort at Connotational Realignment*, LAWFARE (Jan. 29, 2024), https://www.lawfaremedia.org/article/governor-abbott-s-perilous-effort-at-constitutional-realignment.

[119] California v. United States, 104 F.3d 1086 (9th Cir. 1997) (Previous court cases reject the utilization of immigration for an invasion claim: "Additionally, even if the issue were properly within the Court's constitutional responsibility, there are no manageable standards to ascertain whether or when an influx of illegal immigrants should be said to constitute an invasion…" In The Federalist No. 43, James Madison referred to the Invasion Clause as affording protection in situations wherein a state is exposed to armed hostility from another political entity. Madison stated that Article IV, § 4 serves to protect a state from "foreign hostility" and "ambitious or vindictive enterprises" on the part of other states or foreign nations.); *see* Barber v. Hawaii, 42 F.3d 1185, 1199 (9th Cir. 1994) (dismissing an Invasion Clause claim as a nonjusticiable political question); Robert G. Natelson & Andrew T. Hyman, *The Constitution, Invasion, Immigration, and the War Power of States*, BR. J. AM. LEG. STUDIES 13 (2004) ("Rather, as the Constitution employs the words "invasion" and "invaded," those words denote an unauthorized and uninvited intrusion of any size across a border—including significant unauthorized immigration—where the intrusion causes, or threatens to cause, detriment beyond the fact of the intrusion itself. An invasion need not be armed or even formally organized, although organization does tend to show a link between the intrusion and potential or actual detriment."); Orin Kerr, *District Court Enjoins S.B. 4, the Texas Immigration Enforcement Law*, REASON: THE VOLOKH CONSPIRACY (Feb. 29, 2024), https://reason.com/volokh/2024/02/29/district-court-enjoins-s-b-4-the-texas-immigration-enforcement-law/ ("Texas immigration enforcement law was enjoined in *United States v. Texas* on the premise that the "surges in immigration do not constitute an 'invasion.'"").

[120] United States v. Texas, No. 1:24-CV-8-DAE (W.D. Tex. Feb. 29, 2024), https://www.supremecourt.gov/DocketPDF/23/23A815/302258/20240304174805164_Appendix.pdf ("Finally, to allow Texas to permanently supersede federal directives on the basis of an invasion would amount to nullification of federal law and authority—a notion that is antithetical to the Constitution and has been unequivocally rejected by federal courts since the Civil War.").

[121] U.S. CONST. art. I, § 10, cl. 3 ("No State shall, without the Consent of Congress, lay any Duty of Tonnage, keep Troops, or Ships of War in time of Peace, enter into any Agreement or Compact with another State, or with a foreign Power, or engage in War, unless actually invaded, or in such imminent Danger as will not admit of delay.").

[122] 18 U.S.C. § 2331 ("The term 'act of war' means any act occurring in the course of—declared war; armed conflict, whether or not war has been declared between nations; or armed conflict between military forces of any origin.").

situation where there has been no act of war but rather, when the state is in imminent danger. The government has defined imminent danger in civil contexts through statutes and case law, requiring only an expectation of death or serious physical harm.[123] Imminent danger is more difficult to define in a military setting. The term has an interwoven history with preemptive self-defense and tends to be defined based on specific contexts.[124] The ambiguity of the term is important because historically, cyberattacks have not been classified as armed attacks or acts of war. The Department of Defense Manual states that,

> [o]perations described as 'cyber attacks' or 'computer network attacks,' … are not necessarily 'attacks' for the purposes of applying rules on conducting attacks during the conduct of hostilities. Similarly, operations described as 'cyber attacks' or 'computer network attacks' are not necessarily 'armed attacks' for the purposes of triggering a nation-state's inherent right of self-defense under jus ad bellum.[125]

Considering this Gordian's knot of interpretation, the question remains whether a cyberattack is sufficient to fulfill the Clause's imminent danger or invasion requirement.

Cyberattacks reveal a tension between legal standards of the past and legal standards needed for the future. The effort to distinguish kinetic and soft acts of war is worthwhile because the acts are different in kind, witnessed in their categorization as violent or non-violent. However, differentiating cyberwarfare from kinetic acts of war is fraught when cyberspace usurps more and more space in the "real world." The DoD Manual outlines the type of cyberattack that might trigger traditional laws of war, specifying the need for physical consequences.[126] The conclusion is that labeling cyber operations is tricky business. However, there is some consensus that not all malevolent cyber operations can go unpunished and when a cyberattack meets certain metrics, a country is justified to respond with force.[127]

---

[123] Occupational Safety and Health Act of 1970 § 13(a), 29 U.S.C. § 662(a) (defining "imminent danger" as "... any conditions or practices in any place of employment which are such that a danger exists which could reasonably be expected to cause death or serious physical harm immediately or before the imminence of such danger can be eliminated through the enforcement procedures otherwise provided by this Act.").

[124] Mark L. Rockefeller, *The Imminent Threat Requirement for the Use of Preemptive Military Force: Is it Time for a Non-Temporal Standard*, 33 DENV. J. OF INT'L L. & POL'Y 33 (2004).

[125] DOD MANUAL, *supra* note 24.

[126] *Id.* at 1025 ("Thus, cyber operations may be subject to a variety of law of war rules depending on the rule and the nature of the cyber operation. For example, if the physical consequences of a cyber attack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyber attack would equally be subject to the same rules that apply to attacks using bombs or missiles. Cyber operations may pose challenging legal questions because of the variety of effects they can produce. For example, cyber operations could be a non-forcible means or method of conducting hostilities (such as information gathering), and would be regulated as such under rules applicable to non-forcible means and methods of warfare. Other cyber operations could be used to create effects that amount to an attack and would be regulated under the rules on conducting attacks. Moreover, another set of challenging issues may arise when considering whether a particular cyber operation might be regarded as a seizure or destruction of enemy property and should be assessed as such.").

[127] *Id.* at 1028 ("Cyber operations may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law. For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under jus ad bellum, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes. Similarly, cyber operations that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under jus ad bellum. Other factors, besides the effects of the cyber operation, may also be relevant to whether the cyber operation constitutes a use of force under jus ad bellum.").

This article aims to bring attention to the unanswered questions surrounding cyberwarfare and constitutionally granted state powers. *Could* Section 10 be invoked by California if a cyberattack qualifies as an invasion? Potentially. The crux of the state's war powers is its defensive nature.[128] States cannot declare war on the offensive. They can only protect themselves once attacked. There is a critical line between a state taking protective measures and a state engaging in a defensive war. Yet, defining that line in cyberspace can be tricky. As Roman authorship tells us, *si vis pacem, para bellum*—if you desire peace, prepare for war.[129] States are busy passing laws attempting to establish "reasonable cybersecurity practices."[130] Their concern about data breaches, cybercrime, and other acts by malicious actors including nation-states is reasonable.[131] Yet, while these state laws have varying levels of success, they are merely preventative at best. What happens when a state does all it can to prevent cyberattacks and still finds itself in trouble? The recent DoD Manual outlines examples of cyberattacks that would trigger the laws of war, but this does not answer the question of what kinds of cyberattacks would trigger Section 10.[132]

This article does not aim to provide a framework of what kinds of cyber-attacks would invoke Section 10. Rather, this article is intended to draw attention to the potential utility of a mostly forgotten Constitutional provision. The consequences of states reviving their dormant war powers could be severe, but the absence of federal action is equally consequential. The Founders' magnum opus has kept afloat a democratic experiment for over two hundred years. The need for constant reinterpretation is the text's strength and weakness. The application of textual interpretations to states' rights and cyberspace could shape the future of the United States. This country depends on the ability of states to coexist and collaborate, and the challenge of cyberspace is no exception to this rule. When confronting the growing digitization of warfare, this country might consider revitalizing states' war powers to handle the unknown (letters of marque anyone?).

---

[128] Rob Natelson, *Understanding the Constitution: How States May Respond to Illegal Immigration – Part II*, INDEPENDENCE INSTITTUE.ORG (Jan. 16, 2024), https://i2i.org/understanding-the-constitution-how-states-may-respond-to-illegal-immigration-part-ii/ ("In other words, states may wage defensive, but not offensive, war.").
[129] Adam Roberts, *Si vis pacem, para bellum*, MEDIUM (Apr. 1, 2023), https://medium.com/adams-notebook/si-vis-pacem-para-bellum-a5ad331c0e4.
[130] Scott Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86 (2023) (citing "California's 2020 mandate for mandate for manufacturers of Internet-connected devices" and Ohio who have "elected instead to provide safe harbors which reward companies for investing in a pre-determined list of recognized cybersecurity standards and frameworks.").
[131] *Id.*
[132] DOD MANUAL, *supra* note 24.