2016

Cyberwar, International Politics, and Institutional Design

Daniel Abebe

The University of Chicago Law Review

Volume 83 Winter 2016 Number 1

SYMPOSIUM

Cyberwar, International Politics, and Institutional Design

Daniel Abebe†

In the United States, the breadth of the president's warmaking authority has been governed by the Constitution, the Supreme Court's jurisprudence, and, over time, historical practice; in short, the president's powers are constrained by a well-developed body of US foreign relations law. But the prospect of a new kind of conflict—cyberwar—potentially challenges the existing regulatory regime, which rests on assumptions that are common to traditional, conventional war. For some, the complexities of cyberwar generate new foreign relations–law questions about the president's authority to engage in offensive cyberoperations, and they thus necessitate a new regulatory framework. For others, cyberwar is not meaningfully different from traditional war for purposes of foreign relations law, and the extant regime regulating the president is sufficient. As it currently stands, the debate about the scope of the president's cyberwar authority turns on arguments about cyberwar's similarity or dissimilarity to conventional war.

This Essay argues that any claim about regulating the president's authority to engage in cyberwar requires consideration of the United States' cyberstrategy and the capacity and national interests of the United States' cybercompetitors. For the United States to achieve its foreign policy goals in cyberspace, the president

† Harold J. and Marion F. Green Professor of Law, The University of Chicago Law School. I am grateful to Richard Epstein, Aziz Huq, and the many participants at the Symposium on "National Security: The Impact of Technology on the Separation of Powers" at the University of Chicago Law School for helpful comments and suggestions. I also owe thanks to Max Lesser for his excellent research assistance and *The University of Chicago Law Review* for their outstanding editing and organization of the Symposium. Finally, I would like to acknowledge the support of the George J. Phocas Fund and the Elmer M. Heifetz Fund. All mistakes are mine.

must navigate both the internal constraints from domestic law and the external constraints from international politics. Building on previous work, the Essay provides two models with which to understand internal and external constraints and their consequences on any potential cyberwar regulation. It contends that a framework that does not consider the complex relationship between the two types of constraints might result in a regulatory regime that leaves the president overconstrained and unable to achieve US cyberpolicy goals.

INTRODUCTION

US foreign affairs law regulates the president's warmaking authority. The Constitution, the Supreme Court's foreign affairs precedent, statutory restrictions, and historical practice, considered together and sometimes accompanied by functional considerations, create the judicial and legislative regimes regulating the president. Consideration of these factors will, so the conventional wisdom goes, produce the constitutionally required level of oversight over the president's warmaking activities. In short, the focus is on exclusively domestic, internal constraints on the president. For many, the story stops here.

But this does not get us very far. The conventional wisdom ignores the impact of external constraints on the president as he pursues US foreign policy objectives. In a series of articles,[1] I have argued that to determine the appropriate level of regulation of the president, we need to not only consider the foreign policy goals of the United States but also understand the nature of the international political environment. Most important, we must consider the external constraints that are created by the competing foreign policy goals and strategic interests of potential adversaries. Although the Constitution's text, theories of separation of powers, and institutional competencies are certainly relevant to the analysis, they provide insufficient guidance by themselves. Rather, if we want the president to achieve the United States' foreign policy objectives—whatever they may

---

[1] See generally Daniel Abebe, *The Global Determinants of U.S. Foreign Affairs Law*, 49 Stan J Intl L 1 (2013) (developing a theory of internal and external constraints and a framework with which to understand the impact of international political variables on the president's foreign affairs authority); Daniel Abebe, *Rethinking the Costs of International Delegations*, 34 U Pa J Intl L 491 (2013) (arguing that the United States' influence on the operation of international organizations makes delegations of authority less costly than originally assumed); Daniel Abebe, *One Voice or Many? The Political Question Doctrine and Acoustic Dissonance in Foreign Affairs*, 2012 S Ct Rev 233 (arguing that the one-voice presumption between Congress and the president should vary based on international political variables).

be—we need to know something about the external constraints on the United States in international politics to better calibrate the level of internal constraints on the president.

This key insight is no less salient in the context of regulating the president's cyberwarmaking authority. Recently, the Obama administration formally outlined the United States' Cyber Strategy and, for the first time, described the conditions under which the United States would engage in cyberwarfare.[2] Although the Cyber Strategy declares that the United States, through the president, will comply with international and domestic law, it still contemplates the possibility of cyberwarfare and cyberwarmaking by the president, perhaps even in the absence of specific legislative authorization.[3] The potential for cyberoperations and cyberwar generates an interesting set of questions about the suitability of the traditional foreign affairs understanding of war for a new, technologically complex type of warfare. Is the conventional model perfectly appropriate for the cybercontext? Is new regulation necessary? If so, in what form?

In this Essay, I try to make progress in answering these questions. I argue that the strength of external constraints on the United States in the cyberwar context should affect the way we think about the level of internal constraints (cyberregulation) on the president. The normative claim is that as the external constraints on the United States strengthen, the internal constraints on the president should weaken, and that as the external constraints on the United States weaken, the internal constraints on the president should strengthen. The overall level of constraint on the president is the sum of external and internal constraints, and determining the right level of cyberregulation requires consideration of the dynamic relationship between the two. Failure to appreciate this might result in overconstraint, leaving the president unable to achieve US cyberpolicy goals, or in

---

2 *The Department of Defense Cyber Strategy* *5 (Department of Defense, Apr 2015), archived at http://perma.cc/T7UH-NM3S (noting that, under the direction of the president or secretary of defense, "the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace" or "to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations").

3 Id (specifying that defensive action may be taken in response to cyberattacks resulting in "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States," but qualifying that cyberattacks are to be "assessed on a case-by-case and fact-specific basis by the President and the U.S. national security team").

underconstraint, allowing the president to act without sufficient oversight and potentially creating costs for the United States.

Consideration and categorization of all possible external constraints is certainly well beyond the scope of this Symposium contribution. However, a short list of external constraints includes: international law; the cybercapacity, strategic interests, and foreign policy goals of our potential cyberadversaries, including China, Russia, North Korea, Iran, and various nonstate actors; and the vast array of private sector military, software, and technology companies involved in cybersecurity issues,[4] among other constraints. Although an exhaustive analysis is impossible here,[5] the Essay takes an initial step in considering the range of external constraints on the United States by examining the cybercapacity and strategic interests of China and Russia, with the goal of better understanding the nature of external constraints on the United States. Part I discusses the US regime for regulating the president's foreign affairs authority and the international law rules regulating a state's use of force. Part II applies my framework of internal and external constraints to the cyberwar context and provides some tentative thoughts on the merits of domestic and international cyberregulation.

I. US FOREIGN AFFAIRS LAW, INTERNATIONAL LAW, AND CYBERWAR

International law defines, specifies, and regulates the narrow conditions under which a state can use force against another state. Similarly, the constitutional law of US foreign affairs regulates the way that the United States engages in hostilities, and it divides US warmaking authority between Congress and

---

[4] Professor Ashley Deeks provides a very helpful discussion of the external intelligence and national-security constraints on the president in her Symposium contribution. See generally Ashley Deeks, *Checks and Balances from Abroad*, 83 U Chi L Rev 65 (2016) (discussing the role of foreign intelligence services and corporations in potentially constraining the president in the cybercontext).

[5] For a comprehensive analysis of the national-security issues related to cyberspace, cyberwar, and cyberstrategy, see generally Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (Norton 2015); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (Ecco 2010); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds, *Cyberpower and National Security* (Potomac 2009). For purposes of this Essay, cyberattacks are "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* 68 (Oxford 2014).

the president. Together, both bodies of law shape the legal regulatory framework for the use of force by the United States. What remains unclear, however, is the suitability of this framework, drawn from the conventional-war context, for the potential challenges that cyberwarfare presents. In short, is new legal regulation, whether by statute or treaty, necessary? To make progress on this core question, the sections below briefly describe the current regime.

A. International Law and Cyberwar

The UN Charter, in Article 2(4), restricts the circumstances under which a state may use force or the threat of force against another state.[6] Article 2(4) works in conjunction with Article 51 of the Charter, which provides a narrow exception for the use of force in self-defense in the event of an "armed attack."[7] To illustrate the interaction of these two articles, an offensive cyberattack by State A on State B might violate the "use of force" prohibition in Article 2(4) and, if so, could serve as the basis for State B to exercise its right to self-defense[8] if the cyberattack constituted an "armed attack" under Article 51.[9] Finally, the UN Security Council, under Articles 39, 41, and 42 of the Charter,[10] may permit the use of cyberwar as part of the "measures" or "action[s]

---

6 UN Charter Art 2(4) ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

7 UN Charter Art 51:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

8 A further question is whether State B may use military force in response to a cyberattack.

9 For thoughtful discussion of these issues in the cybercontext, see generally Oona A. Hathaway, et al, *The Law of Cyber-Attack*, 100 Cal L Rev 817 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J Intl L 421 (2011).

10 UN Charter Arts 39, 41–42.

. . . necessary to maintain or restore international peace and security."[11]

The United States has taken the position that cyberattacks may trigger both Article 2(4) and Article 51 of the Charter under certain circumstances. Specifically, "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force" under Article 2(4) and trigger a "national right of self-defense" under Article 51.[12] If a state invokes Article 51, the core principles of the law of armed conflict (LOAC)—*jus in bello* or international humanitarian law, including the requirements of proportionality, military necessity, distinction, and the avoidance of unnecessary suffering—proscribe the exercise of self-defense.[13] Such prohibitions would presumably apply to any self-defense measures taken in response to a cyberattack, just as they do with respect to conventional warfare. Despite the United States' position that the Charter and LOAC apply to cyberattacks, the international legal framework regulating the use of force unsurprisingly corresponds to a more traditional conception of war. At times, the framework is incongruous with the technological complexity of cyberwarfare.

For example, in cyberspace it is unclear what constitutes a weapon, an act of war, or the use of force necessary to trigger UN Charter protections. Perhaps more importantly, the problem of attribution—necessary for a state's invocation of Article 51's self-defense provisions—is exceedingly difficult in cyberspace, or at least much more so than in traditional military conflicts.[14] Further, under international humanitarian law, the principles of proportionality and the distinction between military and nonmilitary targets are harder to apply in the cyberwar context, especially if states choose to respond to cyberattacks with conventional

---

11 UN Charter Art 42.

12 Harold Hongju Koh, *International Law in Cyberspace*, 54 Harv Intl L J Online 1, 4 (2012) (emphasis omitted) (providing examples of Article 2(4) violations, including "(1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes").

13 For a summary of these *jus in bello* limitations and a discussion of their application in the context of cyberattacks, see Michael Gervais, *Cyber Attacks and the Laws of War*, 30 Berkeley J Intl L 525, 562–75 (2012).

14 See Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 AF L Rev 167, 193 (2012) ("Given the inherent anonymity of the technology involved, attribution of a cyber attack can be time-consuming and [it can be] difficult to conclusively identify the entity initiating or directing the attack.").

military force (or to counter military force with cyber-operations).[15] Cyberattacks on the military infrastructure of telecommunications networks in cyberspace might have severe consequences on civilian networks, further complicating assessments of proportionality and distinction even for states making good faith efforts to comply with international humanitarian law.[16] Finally, in the absence of an international cyberspace treaty[17] to define the relevant terms, many of the technical questions regarding the fit between the Charter and international humanitarian law on one hand, and the complexity of cyberwar on the other, remain unanswered.

B. US Law and Cyberwar

As the Section below discusses, the possibility of cyberwar generates a number of complicated foreign relations–law questions regarding the extent of the president's independent authority to engage in cyberwarfare. Such questions have become increasingly important as the Obama administration begins to outline the United States' approach to cyberoperations and the breadth of the president's authority to carry out cyberattacks. For example, in mid-April 2015, Secretary of Defense Ashton Carter announced the United States' Cyber Strategy, which states that the United States will use cyberwarfare as a part of offensive military operations, in retaliation for cyberattacks, and as part of covert actions against potential state threats. The Cyber Strategy specifically describes China, Russia, North Korea, and Iran as "[k]ey [c]yber [t]hreats" and "[p]otential adversaries,"[18]

---

[15] See Gervais, 30 Berkeley J Intl L at 565–69 (cited in note 13) ("The international humanitarian law definition of combatant is an awkward fit for cyberspace."). See also id at 571–73 (noting that "[t]he proportionality analysis of a cyber attack must always be considered on a case-by-case basis" and describing the difficulty in determining "whether a cyber attack can meet the necessary requirements to be considered lawful").

[16] See Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, in Michael N. Schmitt and Brian T. O'Donnell, eds, *Computer Network Attack and International Law* 219, 227–28 (Naval War College 1999). See also Gervais, 30 Berkeley J Intl L at 568–69 (cited in note 13) ("A harder determination to make is whether it is unlawful to attack dual-use objects that serve both civilian and military purposes."); Sheng Li, Note, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38 Yale J Intl L 179, 209 (2013) (arguing that proportionality "may favor [ ] targeting enabling infrastructure" as a good faith defensive response to a cyberattack and using the case of the 2007 cyberattacks against Estonia as an illustration).

[17] For a discussion about the obstacles to reaching an international cybertreaty, see generally Michael J. Glennon, *The Dark Future of International Cybersecurity Regulation*, 6 J Natl Sec L & Pol 563 (2013).

[18] *The Department of Defense Cyber Strategy* at *9 (cited in note 2).

and it pledges that the United States will engage in cyberoperations "[i]n a manner consistent with [American] and international law . . . to deter attacks and defend the United States against any adversary."[19] Finally, it suggests that the United States might, under certain circumstances, engage in preemptive cyberoperations: "[T]he United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, *or to disrupt an adversary's military systems to prevent the use of force against U.S. interests*."[20] Most relevant here, the Cyber Strategy neither specifically identifies the precise legal basis for the president to engage in offensive cyberoperations without specific authorization from Congress, nor clearly suggests that the existing constitutional and statutory framework already provides such authority.

1. US war powers.

Very briefly, the Constitution provides the basic structure for understanding the national government's foreign affairs and warmaking authority. Congress is formally assigned the bulk of the foreign affairs authority in Article I; most salient for our purposes are the powers to declare war,[21] raise and support an army,[22] and regulate the armed forces.[23] In contrast, the president has a narrower grant of authority related to war, specifically the Commander-in-Chief Clause in Article II.[24] Moreover, Congress can limit—and has limited—the president's warmaking power at times through the use of its appropriations authority[25]

---

19 Id at *2.

20 Id at *5 (emphasis added).

21 US Const Art I, § 8, cl 11.

22 US Const Art I, § 8, cl 12.

23 US Const Art I, § 8, cl 14.

24 US Const Art II, § 2, cl 1.

25 During the Vietnam War, Congress restricted President Richard Nixon's expansion of the war to Cambodia by denying funds for the introduction of ground-combat troops. See Special Foreign Assistance Act of 1971 § 7(a), Pub L No 91-652, 84 Stat 1942, 1943. Similarly, Congress attempted to constrain the president and limit US involvement with the contras. See, for example, Intelligence Authorization Act for Fiscal Year 1984 § 108, Pub L No 98-215, 97 Stat 1473, 1475 (limiting funding for the contras from any source to $24 million).

and through foreign affairs legislation,[26] most prominently the War Powers Resolution.[27]

Despite the limited number of enumerated grants in Article II, the president is generally considered the leading actor in foreign affairs[28] and plays the primary role in developing US foreign policy.[29] The Supreme Court's broad interpretations of Article II,[30] the accumulated historical practice in foreign affairs,[31] the perceived congressional acquiescence to the executive,[32] and the functional advantages of the executive[33] have all contributed to the president's dominant position in foreign affairs.

Although some of the president's authority in foreign affairs stems from Congress's broad statutory delegations of power,[34]

---

26 See, for example, War Crimes Act of 1996, Pub L No 104-192, 110 Stat 2104, codified as amended at 18 USC § 2441; *Little v Barreme*, 6 US (2 Cranch) 170, 177–78 (1804) (holding that the president cannot ignore congressional restrictions on the capture of vessels during war).

27 Pub L No 93-148, 87 Stat 555 (1973), codified as amended at 50 USC § 1541 et seq (limiting the president's ability to commit the United States to war without prior congressional authorization and requiring the president to disclose his activities to Congress, among other restrictions).

28 See, for example, Eric A. Posner and Adrian Vermeule, *The Executive Unbound: After the Madisonian Republic* 174 (Oxford 2010) ("Executives have always had the leading role in foreign affairs because of the fast-changing nature of international relations and the importance of secrecy and unity."); Eric A. Posner and Cass R. Sunstein, Chevron*izing Foreign Relations Law*, 116 Yale L J 1170, 1202 (2007) ("Courts sometimes say that the executive has the primary foreign relations power."); Harold Hongju Koh, *The National Security Constitution: Sharing Power after the Iran-Contra Affair* 69 (Yale 1990) (noting disapprovingly that, "[a]s it has evolved, the National Security Constitution assigns to the president the predominant role" in the process of making and validating foreign policy decisions).

29 Curtis A. Bradley and Jack L. Goldsmith, *Foreign Relations Law: Cases and Materials* 175 (Wolters Kluwer 5th ed 2014) ("In practice, the Executive Branch exercises a virtual monopoly over formal communications with foreign nations and also plays a lead role in announcing U.S. foreign policy.").

30 See, for example, *United States v Curtiss-Wright Export Corp*, 299 US 304, 319 (1936) ("The President is the constitutional representative of the United States with regard to foreign nations.").

31 See Posner and Sunstein, 116 Yale L J at 1202 (cited in note 28) ("[T]he underlying justifications [for deference to the executive in foreign relations] are often less textual than functional, based on traditional practices and understandings.").

32 See Derek Jinks and Neal Kumar Katyal, *Disregarding Foreign Relations Law*, 116 Yale L J 1230, 1234 (2007) (noting "the trend of [the executive] circumventing Congress in key decisions involving war powers").

33 See Posner and Sunstein, 116 Yale L J at 1202 (cited in note 28) ("[T]he executive has expertise and flexibility, can keep secrets, can efficiently monitor developments, and can act quickly and decisively; the other branches cannot.").

34 See, for example, Act of Dec 28, 1977 §§ 201–08 ("International Emergency Economic Powers Act"), Pub L No 95-223, 91 Stat 1625, 1626–29, codified as amended at 50 USC §§ 1701–06 (granting the president the power to "investigate, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use,

the president has historically exercised some independent authority in the warmaking context. Both *Durand v Hollins*[35] and the *Prize Cases*[36] stand for the proposition that the president has the independent authority both to protect US citizens and property abroad[37] and to repel attacks and invasions.[38] Much more recently, Presidents Bill Clinton and Barack Obama arguably engaged in offensive uses of force during the 1999 Kosovo bombing campaign and the 2011 Libya intervention, respectively, without complying with the specific congressional-authorization requirement in the War Powers Resolution.[39] Finally, while there is a general consensus that congressional authorization is required for the United States to go to war (understood as a long-term engagement in offensive military activities),[40] once hostilities have commenced, the Commander-in-Chief Clause provides the president with formal authority over the conduct of hostilities. Against this backdrop of presidential warmaking authority, the salient question is whether cyberoperations and cyberwar are sufficiently distinct from conventional military operations and war to justify revision of the existing legal framework governing the president's power in this arena.

2. Conventional war and cyberwar.

We can imagine several different perspectives on this question, ranging from the claim that cyberwar is no different than traditional war for purposes of the president's warmaking authority, to the claim that cyberwar could be so damaging that it warrants greater scrutiny of the president's activities. For example,

---

transfer, withdrawal, transportation, importation or exportation" of foreign property, among other powers).

35 8 F Cases 111 (CC SDNY 1860).

36 67 US (2 Black) 635 (1862).

37 *Durand*, 8 F Cases at 112 (holding that the president has the inherent authority to protect Americans abroad).

38 *Prize Cases*, 67 US (2 Black) at 666 (holding that the Commander-in-Chief Clause provided President Abraham Lincoln with the necessary authority to initiate a blockade during the Civil War).

39 See Geoffrey S. Corn, *Clinton, Kosovo, and the Final Destruction of the War Powers Resolution*, 42 Wm & Mary L Rev 1149, 1154 (2001) ("Operation Allied Force . . . continue[d] beyond sixty days without express statutory authorization, in apparent contravention of the War Powers Resolution."); Judah A. Druck, Note, *Droning On: The War Powers Resolution and the Numbing Effect of Technology-Driven Warfare*, 98 Cornell L Rev 209, 210 (2012) (noting that Obama "stood firmly behind his decision to intervene in Libya without consulting Congress").

40 See Curtis A. Bradley and Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv L Rev 2047, 2057 (2005).

one view is that cyberwarfare is potentially more catastrophic, secretive, and dynamic than conventional warfare and that it consequently requires more oversight. Cyberwarfare has the unique capacity to generate "enormous consequences for the security and other interests of the United States,"[41] which may justify a greater role for Congress in formulating cyberpolicy.[42]

A similar view suggests that the United States should regulate cyberoperations under the covert action statute,[43] which formally defines the scope of permissible US covert actions, establishes a strict approval process for the president, and creates a reporting regime to ensure that Congress is regularly informed of any covert actions.[44] The statute is preferable to the legal framework for military action because "[c]yberattacks' key attributes—remote access, unpredictable effects, and difficulty of attribution—can result in fundamentally different legal problems than conventional weapons attacks."[45] Some worry that the statute, however, excludes "traditional . . . military activities or routine support to such activities"[46] from the definition of covert action, meaning that the president could classify offensive cyberoperations as traditional military activities and avoid congressional oversight.[47] Other proposals include measures that "would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons" and that "would restrict potential executive branch actions that seem—as a matter of policy—particularly unwise."[48] Though these perspectives

---

41 Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J Natl Sec L & Pol 155, 162 (2010).

42 Id at 162–64.

43 Intelligence Authorization Act, Fiscal Year 1991 § 602(a)(2), Pub L No 102-88, 105 Stat 429, 442–44, codified as amended at 50 USC §§ 3091–93.

44 For a more detailed discussion of the covert action statute, see William J. Daugherty, *Approval and Review of Covert Action Programs since Reagan*, 17 Intl J Intell & Counterintell 62, 66–67 (2004). See also generally W. Michael Reisman and James E. Baker, *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law* (Yale 1992).

45 Aaron P. Brecher, Note, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 Mich L Rev 423, 430 (2012). The Obama administration's Cyber Strategy moves away from a covert action model. See David E. Sanger, *Pentagon Announces New Strategy for Cyberwarfare* (NY Times, Apr 23, 2015), archived at http://perma.cc/CF2N-C32X.

46 50 USC § 3093(e)(2).

47 See, for example, Dycus, 4 J Natl Sec L & Pol at 161–62 (cited in note 41); Brecher, Note, 111 Mich L Rev at 435–36 (cited in note 45).

48 Dycus, 4 J Natl Sec L & Pol at 167 (cited in note 41). For more discussion of offensive cyberoperations, see generally Eric Lorber, Comment, *Executive Warmaking Authority*

by no means reflect the full range of potential policy proposals for the regulation of cyberwar and cyberoperations, they are consistent in structure with the recurring debate about the proper balance between the president and Congress in foreign affairs—that is, between providing the president with sufficient flexibility to address national-security issues and ensuring that Congress can meaningfully exercise its oversight function.

At this stage, it becomes clear that the rapidly evolving cyberregulation debate is incomplete. By focusing exclusively on internal factors, the debate leaves out the external variables that shape the president's options in achieving the United States' cyberpolicy goals, whatever they may be. More concretely, this Essay argues that we cannot determine the proper level of cyberregulation—or even determine whether new regulation is necessary—without at the very least considering the United States' cybercapacity relative to other states, both today and over time; the strategic interests and the level of internal cyberregulation of potential adversaries; and the prospects for and the likely efficacy of international cyberregulation, among other factors. In other words, US cyberregulation, in whatever form, must consider not only the *domestic* constitutional and statutory issues relating to congressional oversight of the president (internal constraints) but also the *international* factors that limit the United States' cyberwarfare capacity (external constraints).

In Part II, I discuss my general framework for considering internal and external constraints and apply it to the cyberregulation context.

II. STRATEGIC INTERESTS AND CYBERWAR REGULATION

Scholars might examine the relevant legal authorities and conclude that the constitutionally required level of cyberwar regulation permits the president to independently exercise the United States' defensive cyberwar capabilities, but that it mandates specific authorization from Congress for any preemptive or offensive cyberoperations.[49] It might be argued that such a cyberregime is

and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?, 15 U Pa J Const L 961 (2013).

[49] See Bradley and Goldsmith, 118 Harv L Rev at 2057 (cited in note 40) (noting that "[m]any war powers scholars argue that the President is constitutionally required to obtain some form of congressional authorization before initiating significant offensive military operations," but also noting that these scholars "do not typically argue that Congress's authorization must take the form of a formal declaration of war").

consistent with separation of powers in that it not only captures the president's need for flexibility in defending the United States but also ensures that Congress can exercise oversight capacity, shape cyberpolicy, and prevent potential abuse. Though this regime might satisfy constitutional prerequisites for striking a balance between flexibility and oversight in cyberregulation, there is no reason to believe that the regime provides the president with the necessary latitude to pursue the United States' strategic interests in international politics. I argue that this regime is unlikely to produce cyberregulation that is tailored to the United States' cyberpolicy needs, because it does not consider the relationship between the president's pursuit of US interests and the external constraints on the United States imposed by its potential adversaries—China and Russia.

A. A Framework for Cyberregulation and Institutional Design

At issue here is determining the proper level of regulation of the president's exercise of offensive cyberwarmaking authority. For guidance, we can look to the Constitution, Congress's foreign affairs–related statutes, and historical practice, and we can further consider the relative competencies and incentives of the president and Congress. After evaluating all of these factors, we might conclude that a particular form of regulation is legally required. But in arriving at this conclusion, we are looking solely at domestic, internal sources of law to establish the appropriate level of cyberregulation.

With that in mind, it is unlikely that a narrow examination of domestic variables will produce a cyberregulatory regime that permits the United States to achieve its cyber-related foreign policy goals. Whatever the United States' strategic objectives (this Essay is agnostic on what they should be), the main purpose of any cyberregulatory regime is to provide the president with the necessary latitude to achieve US interests, while allowing congressional oversight to prevent the president from adopting policies that impose costs on the United States. Of course, we should start the analysis by considering the Constitution, statutes, and precedent, but we must also understand the external environment in which the United States pursues its foreign policy goals. Most importantly, we need to evaluate the obstacles, adversaries, and constraints that the United States, through the president, faces in realizing its cyberstrategy objectives.

For example, let's assume that the United States is the world's predominant cyberpower. Call this Model One. In this model, the United States possesses the most-advanced offensive-cyberwarfare capacity and also maintains formidable cyber-defenses. In short, the United States is the sole "cyber-superpower" and, acting through the president, is well-placed to pursue and achieve its cyberpolicy goals. And since potential adversaries like China and Russia cannot compete with the United States' cybercapacity, the external constraints on the president (and the United States) from international politics are weak. In this stylized example, the president is free from external political constraints and is limited by only internal legal constraints.

In contrast, let's assume that the United States is one of three evenly matched world cyberpowers, including China and Russia, with other states like North Korea and Iran rapidly improving their cybercapacities. Call this Model Two. In this model, the United States, China, and Russia are aggressively competing for cyberdominance and have the capacity to engage in offensive cyberoperations. Here, the United States, through the president, will encounter much more significant obstacles in its pursuit of the United States' cyberpolicy goals because it will have to contend with powerful adversaries who likely have competing policy objectives. More concretely, China, Russia, North Korea, and Iran represent strong external constraints on the United States and the president.

What are the takeaways? First, there is no reason to believe that the cyberregulatory regime that is appropriate for Model One is also suitable for Model Two. The United States is the sole cybersuperpower in Model One but only one of several competing cyberpowers in Model Two. Given the variation in the United States' cyberpower in the two models, we must calibrate our internal cyberregulation in light of the external constraints that cabin the president's pursuit of the United States' cyberpolicy goals. Stated simply, the cyberpower capacities of potential adversaries reflect the strength of external constraints on the United States, and any cyberregulation must consider these costs, along with the relevant legal authorities, to determine the appropriate level and type of cyberregulation.

Second, whatever you think the optimal level of total restraint should be—again, this Essay takes no position on that question—the strength of internal constraints on the president should vary with the strength of external constraints on the

United States. As external constraints on the United States strengthen—perhaps an adversary with competing interests becomes a cybersuperpower—the internal constraints on the president should weaken. Similarly, as external constraints from our adversaries weaken, the internal constraints on the president should strengthen. Why? A combination of strong internal and external constraints might result in overconstraint, leaving the president unable to achieve US cyberpolicy goals, while weak internal and external constraints might result in underconstraint, permitting the president to act without sufficient oversight and potentially creating costs for the United States.[50]

How would this balance work in practice? Ideally, one would have a fully developed theory of state behavior in cyberspace[51]—akin to international relations theories of state behavior in international politics—to identify the cyber-related variables that are relevant for assessing the strength of external constraints on the United States. Policymakers would then incorporate the results of this assessment into their calculus in calibrating the level of cyberregulation that properly balances the president's need for flexibility in ensuring US national security and Congress's oversight and monitoring prerogatives. Unfortunately, such a theory—and the necessary command of cybertechnology—is well beyond the scope of this Essay. But we still can look to more-traditional measures of state power to provide some preliminary guidance in assessing the cyberenvironment. The cyberbudgets and cyberincentives of the United States and its potential adversaries, to name just two factors, might shed light on the nature of the external constraints on the United States in international politics.

1. Cyberwar capacity: the United States, China, and Russia.

Let's begin by considering the United States' cyberoperations capacity relative to potential adversaries. To keep the discussion brief, I focus on China and Russia. Of course, the analysis here is speculative; neither China nor Russia officially

---

50 For a more complete elaboration of this theory, see Abebe, 49 Stan J Intl L at 37–50 (cited in note 1).

51 Stuart H. Starr takes a tentative step in developing such a theory. See generally Stuart H. Starr, *Toward a Preliminary Theory of Cyberpower*, in Kramer, Starr, and Wentz, eds, *Cyberpower and National Security* 43 (cited in note 5) (outlining the author's "initial effort to develop a theory of cyberpower").

(or fully) discloses its cyberoperations potential, and any evaluation of a state's true cybercapacity requires a strong command of the technical aspects of cyberoperations. That said, we can make incremental progress by examining publicly available information and expert assessments.

The United States Cyber Command ("CYBERCOM") is the centralized command structure charged with leading US cyberoperations.[52] As part of the Department of Defense, CYBERCOM's budget totaled some $447 million for the 2014 fiscal year[53]—part of a general "cyberwarfare budget [that] has grown from $3.9 billion in 2013 to $4.7 billion in 2014 and an estimated $5.1 billion in 2015."[54] CYBERCOM was expected to have a staff of six thousand people by 2016,[55] divided into one hundred teams responsible for "defending military networks, damaging the capabilities of enemy networks[,] and helping to defend the nation's infrastructure"[56] while also achieving the deterrence goals outlined in the Cyber Strategy. The US cyberwarfare budget was a small component of the United States' overall military budget of almost $620 billion for fiscal year 2014.[57] But since the overall size of the US military budget far exceeds the budgets of China and Russia—their combined military expenditures are less than half of the US budget[58]—the United States has the capacity to shift more resources to cyberwarfare than its adversaries can. If the United States' resource advantage in overall military expenditures can be replicated and maintained in the cybercontext, the United States would presumably want to maximize that advantage rather than curtail it.

---

52 *U.S. Cyber Command* (Strategic Command, Mar 2015), archived at http://perma.cc/ZTB8-EKFV.

53 Brian Fung, *Cyber Command's Exploding Budget, in 1 Chart* (Wash Post, Jan 15, 2014), archived at http://perma.cc/B9X7-M8QF.

54 Maggie Ybarra, *Cyber Command Investment Ensures Hackers Targeting U.S. Face Retribution* (Wash Times, Dec 22, 2014), archived at http://perma.cc/72TP-6PVL.

55 Ellen Nakashima, *U.S. Cyberwarfare Force to Grow Significantly, Defense Secretary Says* (Wash Post, Mar 28, 2014), archived at http://perma.cc/LSQ8-HRL6.

56 Jim Michaels, *Pentagon Expands Cyber-Attack Capabilities* (USA Today, Apr 21, 2013), archived at http://perma.cc/47HN-4LS8.

57 Office of the Under Secretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2015* *6 (Department of Defense, Apr 2014), archived at http://perma.cc/7JV9-ASSU.

58 See Richard Norton-Taylor, *Eastern Europe Is Boosting Military Budgets, but US Is Still the Big Spender* (The Guardian, Apr 13, 2015), archived at http://perma.cc/M6HD-YT6S ("The US defence budget amounted to $610bn (£415bn) last year, compared with China's estimated $216bn and Russia's estimated $84.5bn.").

Although the United States' cyberwarfare expenditures are growing, it is unclear how the United States' cybercapacity compares with the cybercapacities of its two largest potential adversaries, China and Russia. According to the Cyber Strategy, China and Russia are viewed as arguably the United States' most serious cybercompetitors.[59] Although trees have been felled with documentation of Chinese cyberattacks on American companies,[60] only in 2015 did China finally disclose the existence of an advanced cyberwar infrastructure that, according to one cyberexpert, is divided into military, civilian, and external entities, each "responsible for targeting American companies to steal their secrets."[61] Unsurprisingly, China's cyberwarfare budget is almost impossible to determine, but one estimate suggests that China's budget is "in the billions, nationwide, and certainly in the hundreds of millions within the Chinese military."[62] China's overall military budget was estimated to be around $216 billion for 2014,[63] meaning that it has significant resources to devote to cyberoperations if it so chooses.

Russia, unsurprisingly, poses similar challenges. According to a 2010 statement by General Keith Alexander, former director of the NSA and head of CYBERCOM, Russia was a "near peer" of the United States in cybercapacity, engaging in offensive cyberoperations most recently in Crimea in 2014 and in Georgia in 2008.[64] Later in 2014, with an initial outlay of $500

---

59 *The Department of Defense Cyber Strategy* at *9 (cited in note 2). See also Franz-Stefan Gady, *Russia Tops China as Principal Cyber Threat to US* (The Diplomat, Mar 3, 2015), archived at http://perma.cc/LXS3-AT4Q; Declan McCullagh, *China's Cyberwar: Intrusions Are the New Normal (FAQ)* (CNET, Feb 19, 2013), archived at http://perma.cc/GV5N-9LNX ("The most remarkable aspect of a new and deeply troubling report about network intrusions originating in China is how commonplace they've become. They're no longer a rare occurrence: A single Shanghai-based hacking organization has reportedly compromised at least 141 companies across 20 industries.").

60 See McCullagh, *China's Cyberwar* (cited in note 59); David E. Sanger, David Barboza, and Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking against U.S.* (NY Times, Feb 18, 2013), archived at http://perma.cc/TE9W-3JTX:

> A growing body of digital forensic evidence—confirmed by American intelligence officials who say they have tapped into the activity of the [Chinese] army unit for years—leaves little doubt that an overwhelming percentage of the attacks on American corporations, organizations and government agencies originate in and around the white tower.

61 Shane Harris, *China Reveals Its Cyberwar Secrets* (The Daily Beast, Mar 18, 2015), archived at http://perma.cc/BG42-RMKE.

62 Bill Gertz, *China Sharply Boosts Cyber Warfare Funding* (The Washington Free Beacon, Apr 1, 2015), archived at http://perma.cc/9UQX-APS4.

63 Norton-Taylor, *Eastern Europe Is Boosting Military Budgets* (cited in note 58).

64 Harris, *China Reveals Its Cyberwar Secrets* (cited in note 61).

million, the Russian Ministry of Defense started recruiting "young programmers and IT experts" to strengthen cyberwar capacity in the Russian army and develop its own cyber-command.[65] In 2015, Director of National Intelligence James Clapper testified before Congress that "the Russian cyber threat is more severe than we had previously assessed," and other independent experts have characterized Russian cyberpower as "underestimated."[66] Russia's military budget for 2014 was approximately $85 billion[67]—significantly smaller than the United States' and China's budgets—but its technological sophistication might make up for its shortfall in resources.[68]

At bottom, although the United States appears to have a more advanced cyberoperation infrastructure (CYBERCOM seems to be the model that states are emulating) and greater resources to invest in cyberoperations, it is unclear whether these advantages easily translate into a significant advantage in overall cyberpower relative to China and Russia. In fact, the concern in the United States is that cyberattacks are growing in frequency and creating greater damage, "cost[ing] the U.S. economy as much as $400 billion a year."[69] Admiral Michael Rogers, current director of the NSA and CYBERCOM, claims that cyberspace tensions today resemble superpower tensions at the beginning of the Cold War, suggesting that the United States, China, and Russia are aggressively pursuing cyberpower dominance.[70]

2. Strategic interests: the United States, China, and Russia.

For the United States, offensive cyberoperations might serve as a low-cost complement to more-expensive conventional

---

65 Eugene Gerden, *$500 Million for New Russian Cyber Army* (SC Magazine UK, Nov 6, 2014), archived at http://perma.cc/N6FE-XD88 ("[T]he Russian government plans to accelerate training of programmers, mathematicians, engineers, cryptographer[s], communicators[,] interpreters and other staff, who will be asked to sign a contract for service in [the] Russian army.").

66 Gady, *Russia Tops China as Principal Cyber Threat to US* (cited in note 59).

67 Norton-Taylor, *Eastern Europe Is Boosting Military Budgets* (cited in note 58).

68 See Gady, *Russia Tops China as Principal Cyber Threat to US* (cited in note 59) ("Russia is singled out as one of the most sophisticated nation-state actors in cyberspace.").

69 Anthony Capaccio and Chris Strohm, *Cyberspace Conflict Growing More Destructive, NSA's Chief Says* (Bloomberg, Mar 3, 2015), archived at http://perma.cc/6WMC-LXEX.

70 Id ("'I liken our historical moment to the situation that confronted the U.S. early in the Cold War, when it became obvious that the Soviet Union and others could build hydrogen bombs and the superpower competition showed worrying signs of instability,' Rogers said in his testimony.").

warfare under certain circumstances.[71] At present, a wide range of strategic factors requires the United States to project power and defend national interests at a global level. These factors include the breadth of the United States' treaty obligations and political commitments, the rise of China, the threat from states like Iran and North Korea, security challenges in the Middle East, and Russian aggression on the European periphery. To the extent that the United States' cyberwarfare tools can deter the use of military force by its adversaries or simply reduce potential fatalities for US citizens and foreign civilians, they might justify expanding the president's cyberwar capacity rather than restricting it.

Conversely, the United States also has the most to lose from failing to develop a comprehensive cyberstrategy.[72] Put bluntly, the United States has more public and private sector assets to defend than either of its main adversaries. US technology companies,[73] large military contractors,[74] and financial services firms[75] are more likely to be the targets of state-sponsored cyberattacks—and espionage—than similar companies in China

---

[71] See David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks against Iran* (NY Times, June 1, 2012), archived at http://perma.cc/RYW7-MYBC ("Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.").

[72] See id:

> In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

[73] See McCullagh, *China's Cyberwar* (cited in note 59):

> Google may have been the first major U.S.-headquartered company to disclose the breadth and persistence of attacks originating in China. Intruders managed to compromise the Gmail accounts of human rights workers and foreign journalists working in Beijing. Google's disclosure came in a January 2010 blog post, with reports soon following that said Adobe, Yahoo, Juniper Networks, Symantec, Northrop Grumman, and Dow Chemical had also been among the 34 companies targeted.

[74] See Mike Lennon, *Lockheed: Attackers Went Quiet after APT1 Report Exposed Chinese Hackers* (SecurityWeek, Aug 14, 2014), archived at http://perma.cc/JYX6-NKUJ (noting that Lockheed executives confirmed that there was an "immediate decrease in [cyber] attacks" after the release of a report describing Chinese cyberespionage).

[75] See Emily Glazer and Danny Yadron, *J.P. Morgan Says About 76 Million Households Affected by Cyber Breach* (Wall St J, Oct 2, 2014), archived at http://perma.cc/ZX4Z-P5GU (confirming that seventy-six million people had their contact information stolen, "including names, email addresses, phone numbers and addresses").

and Russia. For illustrative purposes, one could imagine that a serious cyberattack on the United States' telecommunications or banking infrastructure could create significant economic consequences, while a similar cyberattack on North Korea, Iran, or even Russia might not be as damaging, even in relative terms.

Both China and Russia also want to deploy their offensive cybercapabilities in their respective spheres of interest—in China's case, the South China Sea and Taiwan, while in Russia's case, Eastern Europe and the former Soviet periphery.[76] Similarly, China and Russia presumably have interests in continuing to engage in cyberespionage to gain access to US technology and intellectual property, from both American companies and the US government.[77] At the same time, China and Russia want to deny US offensive cyberoperations against their militaries and other targets. Since in theory China and Russia might not have as many assets to defend, the United States might be able to concentrate its cyberresources on specific targets of value. Finally, it is not clear that China or Russia would want to attempt a cyberattack that constitutes a use of force (something akin to a conventional attack) against the United States, since there is no guarantee of success and the likelihood of a cyberresponse is real.

B. Domestic or International Regulation?

Although the preceding Section represents a superficial examination of the cybercapacity and strategic interests of the United States, China, and Russia, it does provide some guidance on how to think about the merits of both US cyberregulation and an international cybertreaty.

1. US cyberregulation.

In light of the current threat environment, it appears that the United States' interest is in maximizing its cybercapacity and ensuring flexibility to engage in offensive and defensive cyberoperations whenever necessary. By most accounts, the United States does not have an overall cybercapacity that dramatically outstrips its main potential adversaries (China and

---

[76] See Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13 J Internet L 22, 24 (Feb 2010).

[77] See, for example, Hathaway, et al, 100 Cal L Rev at 829 (cited in note 9) (describing Chinese cyberespionage against Google and "other major Internet technology companies" that resulted in the theft of intellectual property and raised suspicions that "at least one purpose of the attack . . . was to monitor U.S. government officials' emails").

Russia),[78] and the United States has the most cyberassets to defend. Moreover, although the United States is ramping up its cybercapacity, China and Russia are doing the same; the United States, as Rogers has noted, is in the midst of a cyber–arms race.[79] To use the illustrative example provided earlier, the United States is operating in Model Two[80]—a world with several competing cyberadversaries. In such a world, strong internal constraints on the president are inapposite, as the United States is already dealing with strong external constraints from China and Russia. This situation is exacerbated by the fact that China and Russia do not have meaningful internal constraints—that is, constraints imposed by law—on their respective capacities to exploit public and private sector cyberresources to engage in cyberoperations against the United States.[81] Overall, the United States faces strong external constraints from relatively evenly matched adversaries (China and Russia) who are free from domestic constraints (of the legal variety). In this environment, for the United States to achieve its cyberpolicy goals, the president will likely need more flexibility—or weak internal constraints—within any cyberregulatory regime.

2. International cybertreaty.

Although there exists a well-developed international law framework regulating the use of force by states, it is too early to tell whether the United States, China, and Russia would truly support an international cybertreaty (whatever its details). Even beyond the difficulties in defining relevant terms, determining attribution for cyberattacks, monitoring state behavior, and imposing sanctions for violators, the United States, China, and Russia might want more time to develop their cybercapacities—and determine their relative strengths and weaknesses—before agreeing to a regime that might limit their abilities to exploit a potential cyberadvantage. If we are indeed at an early stage of a cyber "Cold War," the United States, China, and Russia would likely consider an international cybertreaty only after

---

78 See Gady, *Russia Tops China as Principal Cyber Threat to US* (cited in note 59).

79 See Cassandra M. Kirsch, *Science Fiction No More: Cyber Warfare and the United States*, 40 Denver J Intl L & Pol 620, 622–23 (2012) ("Politicians and academics alike agree that a treaty would lessen the chance of a real cyber war, arguing the world is now in the early stages of a Cyber Arms Race.").

80 See Part II.A.

81 See Waxman, 36 Yale J Intl L at 456 (cited in note 9).

they have developed sufficient cyberdeterrents or, if you will, second-strike capacities. At that stage, they might feel sufficiently secure in their cybercapacities to negotiate a treaty that would not only limit offensive cyberattacks but also make it harder for other states to develop significant cybercapacities—something akin to a cyberversion of a nuclear nonproliferation agreement. For now, perhaps the limited bilateral agreement[82] between the United States and China on restricting state involvement in cybercrime and commercial espionage—concluded in September 2015—is the best we can do.[83]

CONCLUSION

Considering the strength of external constraints is key to understanding how to set internal constraints, both in conventional war and cyberwar. The goal of this Essay is to provide the first steps in thinking about the application of a model of external constraints in the cybercontext.

The approach outlined here has two other benefits. First, it does not take a position on the content of US cyberpolicy. It simply suggests that if we want the United States to be successful in achieving its cyberprerogatives—whatever they are or should be—then determining the appropriate level of cyberregulation requires some consideration of external constraints. Second, it does not specify the baseline for cyberregulation—it takes no position on whether we already have too much or too little regulation of the president's cyberwar authority. Rather, the approach says that whatever one thinks the baseline is or should be, the strength of external constraints must be part of the analysis.

---

[82] See Julie Hirschfeld Davis and David E. Sanger, *Obama and Xi Jinping of China Agree to Steps on Cybertheft* (NY Times, Sept 25, 2015), archived at http://perma.cc/UQK3-QB3M.

[83] See David E. Sanger, *Limiting Security Breaches May Be Impossible Task for U.S. and China* (NY Times, Sept 25, 2015), archived at http://perma.cc/68UX-EJP4 (suggesting that the United States and China "are still in the beginning phase of a confrontation in cyberspace that will stretch into the next presidency and likely many beyond").