A pandemic, an election, mass protests, Middle East conflicts, cyber warfare, and more: national security is dire to our country now more than ever. Join us to explore the progression and current state of national security law in the United States. Experts in the field will discuss the origins of national security law, how it has transformed following traumatic events such as 9/11, how it has developed in the world of cybersecurity, and what threats we've seen as a result of the COVID-19 pandemic. This free, public event is sponsored by The University of Toledo Law Review.

Table of Contents

Symposium Agenda

9 a.m. – Welcome/Opening

9:30 a.m. – Originalism and National Security Power

Harold J. Krent, professor of law, IIT Chicago-Kent College of Law (Chicago, Ill.)

Erwin Chemerinsky, dean and Jesse H. Choper Distinguished Professor of Law, Berkeley Law (Berkeley, Calif.)

Julian Davis Mortenson, James G. Phillipp Professor of Law, University of Michigan Law School (Ann Arbor, Mich.)

10:45 a.m. – Post-9/11 National Security

Alka Pradhan, lecturer in law, University of Pennsylvania Carey Law School (Philadelphia, Pa.)

Stephen Vladeck, Charles Alan Wright Chair in Federal Courts, University of Texas School of Law (Austin, Texas)

William Banks, professor of law emeritus, Syracuse University College of Law (Syracuse, N.Y.)

Noon – Lunch Break

1 p.m. – Cybersecurity in the Modern Age

Col. Gary Corn, adjunct professor and director of Tech, Law & Security Program, American University Washington College of Law (Washington, D.C.)

Maj. Gen. Charles Dunlap, professor of law and executive director of Center on Law, Ethics and National Security, Duke University School of Law (Durham, N.C.)

Robert Litt, of counsel at Morrison & Foerster (Washington, D.C.)

2:15 p.m. – COVID-19 Threats to National Security

Mary McCord, legal director, Institute for Constitutional Advocacy and Protection (Washington, D.C.)

Javed Ali, Towsley Foundation Policymaker in Residence, University of Michigan Gerald R. Ford School of Public Policy (Ann Arbor, Mich.)

3:30 p.m. – Closing Remarks

Panelist Biographies

ORIGINALISM AND NATIONAL SECURITY POWER

Harold Krent

Harold Krent is a professor of law at the Chicago-Kent College of Law at Illinois Institute of Technology. He graduated from Princeton University and received his law degree from New York University School of Law, where he served as law review notes editor and garnered several awards for excellence in writing. Krent clerked for the Hon. William H. Timbers of the U.S. Court of Appeals for the Second Circuit and then worked in the Department of Justice for the Appellate Staff of the Civil Division, writing briefs and arguing cases in various courts of appeals across the nation. He has been teaching full-time since 1987. His scholarship focuses on the legal aspects of individuals' interaction with the government. Krent has served as a consultant to the Administrative Conference of the United States. He has also litigated numerous cases with students on behalf of indigent prisoners. Krent joined the IIT Chicago-Kent faculty in 1994. He was appointed associate dean in 1997 and interim dean in 2002 before assuming the deanship on Jan. 1, 2003. He continued in his role as dean until July 31, 2019. His book, "Presidential Powers," is a comprehensive examination of the president's role as defined by the U.S. Constitution and judicial and historical precedents.

Erwin Chemerinsky

Erwin Chemerinsky became the 13th dean of Berkeley Law in 2017, when he joined the faculty as the Jesse H. Choper Distinguished Professor of Law. Before assuming this position, he was the founding dean and Distinguished Professor of Law at the University of California Irvine School of Law. Chemerinsky is the author of 12 books and more than 200 law review articles. He writes a regular column for the Sacramento Bee, monthly columns for the ABA Journal and the Daily Journal, and op-eds in newspapers across the country. He frequently argues appellate cases, including in the U.S. Supreme Court. In 2016, Chemerinsky was named a fellow of the American Academy of Arts and Sciences. In 2017, National Jurist magazine named Dean Chemerinsky as the most influential person in legal education in the nation.

Julian Davis Mortenson

Julian Davis Mortenson is the James G. Pillipp Professor of Law at the University of Michigan Law School. He writes on constitutional and international law. His current book project, "The Founders' President" (under contract with Harvard University Press), develops a comprehensive account of presidential power at the American Founding. Mortenson is an award-winning teacher and an active litigator. He regularly litigates complex transnational matters in the U.S. courts and has served as an arbitrator, counsel, and expert witness in a wide variety of commercial and investor-state disputes. He was lead counsel in a pre-*Obergefell* suit that required Michigan to recognize the marriages of more than 300 same-sex couples. He represented discharged military service members challenging the "Don't Ask, Don't Tell" law, and his work as one of the principal drafters of merit briefs in the landmark case *Boumediene v. Bush* secured the right of Guantanamo detainees to challenge their incarceration. Before joining the faculty, Mortenson worked at the law firm WilmerHale, in the President's Office of the UN's International Criminal Tribunal for the former Yugoslavia, and as a law clerk for both Justice David H. Souter and the Hon. J. Harvie Wilkinson III. Before law school, he was a management

consultant with a client portfolio spanning the finance, manufacturing, oil and gas, and information technology industries. Professor Mortenson was salutatorian of his class at Stanford Law School and received an A.B., *summa cum laude*, in history from Harvard College.

POST-9/11 NATIONAL SECURITY

Alka Pradhan

Alka Pradhan is a lecturer in law at the University of Pennsylvania Carey Law School and is human rights counsel at the Guantanamo Bay Military Commissions, representing one of the 9/11 accused. Pradhan has long worked at the crossroads of international human rights and national security. She is a frequent commentator in the media on international law and counterterrorism issues, ranging from force-feeding at Guantanamo Bay to the application of human rights law to detention operations in Iraq. While in private practice at White & Case LLP, Pradhan participated in sovereign litigations and other cases involving public international law, including use of the Alien Tort Statute. In her pro bono practice, she represents asylum-seekers and advises NGOs on litigation before international criminal tribunals and the European Court of Human Rights. Her work was profiled in a New York Times Magazine feature "Alka Pradhan v. Gitmo" in 2017. Pradhan earned her B.A. and M.A. from Johns Hopkins University, her J.D. from Columbia Law School, and an LL.M. from the London School of Economics and Political Science.

Stephen Vladeck

Stephen Vladeck holds the Charles Alan Wright Chair in Federal Courts at the University of Texas School of Law. He is a nationally recognized expert on federal courts, constitutional law, national security law, and military justice. Vladeck has argued multiple cases before the U.S. Supreme Court, the Texas Supreme Court, and lower federal civilian and military courts. He is co-host of the award-winning "National Security Law" podcast. He is CNN's Supreme Court analyst, a co-author of Aspen Publishers' leading national security law and counterterrorism law casebooks, an executive editor of the "Just Security" blog, and a senior editor of the "Lawfare" blog. Vladeck clerked for the Hon. Marsha S. Berzon on the U.S. Court of Appeals for the Ninth Circuit and the Hon. Rosemary Barkett on the U.S. Court of Appeals for the Eleventh Circuit. While a law student, he was the student director of the Balancing Civil Liberties & National Security post-9/11 litigation project. He earned his B.A., *summa cum laude*, in history and mathematics from Amherst College and his J.D. from Yale Law School.

William Banks

William C. Banks is a Board of Advisors Distinguished Professor Emeritus at Syracuse University College of Law. From 2015-16, Banks served as interim dean of the College of Law. Banks was the founding director of the Institute for National Security and Counterterrorism, now the Syracuse University Institute for Security Policy and Law. He is a highly regarded and internationally recognized scholar. His research focuses on constitutional law and national security, counterterrorism, laws of war and asymmetric warfare, cyber conflict, civilian-military relations, and government surveillance and privacy. The subjects of Banks's more than 160 published book chapters and articles range from the military use of unmanned aerial vehicles and the role of the military in domestic affairs to cyberespionage, cyber attribution, and the U.S. Foreign Intelligence Surveillance Court. He is editor of the Journal of National Security Law & Policy and chair of the ABA Standing Committee on Law and National Security.

CYBERSECURITY IN THE MODERN AGE

Col. Gary Corn

Gary Corn is the director for the Tech, Law & Security Program at American University Washington College of Law, where he is an adjunct professor. He is a senior fellow in cybersecurity and emerging threats at the R Street Institute, a member of the editorial board of the Georgetown Journal of National Security Law and Policy, an advisory board director for the Cyber Security Forum Initiative, and the founder and principal of Jus Novus Consulting, LLC. A retired U.S. Army colonel, Corn previously served as the staff judge advocate to U.S. Cyber Command, as a deputy legal counsel to the Chairman of the Joint Chiefs of Staff, the operational law branch chief in the Office of the Judge Advocate General of the U.S. Army, the staff judge advocate to U.S. Army South, on detail as a special assistant U.S. attorney in the District of Columbia, and on deployment to the former Yugoslav Republic of Macedonia as part of the United Nations Preventive Deployment Force and as the chief of international law for Combined Forces Command-Afghanistan. He holds a B.A. in international relations from Bucknell University, an M.A. in national security studies from the U.S. Army War College, a J.D. from George Washington University, and an LL.M. from the Judge Advocate General's Legal Center and School.

Maj. Gen. Charles Dunlap

Gen. Dunlap is a professor of the practice of law and executive director of the Center on Law, Ethics and National Security at Duke University School of Law. His teaching and scholarly writing focus on national security, the law of armed conflict, the use of force under international law, civil-military relations, cyberwar, airpower, military justice, and ethical issues related to the practice of national security law. Dunlap retired from the Air Force in June 2010, having attained the rank of major general during a 34-year career in the Judge Advocate General's Corps. Dunlap previously served as the staff judge advocate at Air Combat Command at Langley Air Force Base in Virginia, Air Education and Training Command at Randolph Air Force Base in Texas, and U.S. Strategic Command in Nebraska. Additionally, he served on the faculty of the Air Force Judge Advocate General School, where he taught various civil and criminal law topics. A prolific author and accomplished public speaker, Dunlap's commentary on a wide variety of national security topics has been published in leading newspapers and military journals.

Robert Litt

Robert Litt is of counsel and co-chair of Morrison & Foerster's global risk and crisis management group. He advises industry-leading organizations on sensitive national security and privacy matters, white collar investigations, and government enforcement actions. He is also an adjunct research scholar in Columbia Law School's National Security Law Program. Before joining Morrison & Foerster, Litt served nearly a decade as the general counsel for the Office of the Director of National Intelligence. He has worked at the Department of Justice as deputy assistant attorney general in the criminal division. He also served as special advisor to the Assistant Secretary of State for European and Canadian Affairs and was an assistant U.S. attorney in the Southern District of New York. In addition to his prolific government service, Litt had an extensive career in private practice as a partner at two global law firms. He holds a B.A. from Harvard College and an M.A. and J.D. from Yale University.

COVID-19 THREATS TO NATIONAL SECURITY

Mary McCord

Mary McCord is the legal director at the Institute for Constitutional Advocacy and Protection (ICAP) and a visiting professor of law at Georgetown University Law Center. At ICAP, McCord leads a team that brings constitutional impact litigation at federal and state courts across a wide variety of areas, including First Amendment rights, immigration, criminal justice reform, and combating the rise of private paramilitaries. McCord was the acting assistant attorney general for national security at the Department of Justice from 2016-17 and principal deputy assistant attorney general for the national security division from 2014-16. Previously, she was an assistant U.S. attorney for nearly 20 years at the U.S. Attorney's Office for the District of Columbia. McCord has written about domestic terrorism, unlawful militia activity, public safety, and the rule of law for publications including the Washington Post, New York Times, Wall Street Journal, Slate, Lawfare, and Just Security. She has appeared on NPR, PBS, CNN, MSNBC, ABC, and other media outlets.

Javed Ali

Javed Ali is a Harry A. and Margaret D. Towsley Foundation Policymaker in Residence at the Gerald R. Ford School of Public Policy at the University of Michigan, where he has been teaching since 2018. Previously, he had over 20 years of professional experience in national security and intelligence issues in Washington, D.C., serving across several departments including the Office of the Director of National Intelligence, the Defense Intelligence Agency, the Department of Homeland Security, and the Federal Bureau of Investigation. While at the FBI, Ali held senior positions on joint duty assignments at the National Intelligence Council, the National Counterterrorism Center, and the National Security Council. He writes and provides commentary across several media sites and platforms, including MSNBC, CBS, CNN, ABC, The New York Times, The Washington Post, The Hill, and Newsweek.

CLE Handouts

ARTICLE: Reviving the Power of the Purse: Appropriations Clause Litigation and National Security Law

June, 2018

Reporter
127 Yale L.J. 2512 *

Length: 10477 words

Author: MCKAYE NEUMEISTER

Highlight

ABSTRACT. The rise of the modern ***national security*** state has been accompanied by a vast expansion of ***executive*** ***power***. Congress's strongest check against unilateral presidential action--the ***power*** of the purse--has so far been ineffective in combating this constitutional imbalance. But developments in legislative standing doctrine may make it possible for congressional plaintiffs to challenge ***executive*** violations of the Appropriations Clause. Those evolutions could enable Congress to use the Appropriations Clause to reassert its role in ***national security*** decision making and restore the constitutional balance the Framers crafted.

Text

[*2515] INTRODUCTION

Since the Founding, war has changed. The ***national security*** challenges we face as a nation today are beyond the comprehension of the Framers. Yet the text of the Constitution remains the same. While Congress has the formal authority to be a significant force in ***national security*** policy making, [1] military conflicts do not occur within the Constitution's battle lines any longer. Instead, in the modern era, the

---

[1] *See* DOUGLAS L. KRINER, AFTER THE RUBICON: CONGRESS, PRESIDENTS, AND THE POLITICS OF WAGING WAR 39 (2010) ("On parchment at least, Congress has more than enough tools at its disposal to serve as a strong check on presidential ***power*** in the military arena.").

President has the ability to initiate military conflicts without prior congressional authorization. [2] Congress is left playing catch-up, attempting to regulate military operations already underway. [3] The war ***power*** has thus shifted from Congress to the President, [4] and congressional attempts to constrain the President often go unheeded. [5] As Professors Bruce Ackerman and Oona Hathaway have observed, "[t]here is a pressing need for institutional reform that allows Congress to restore our endangered balance of ***powers***" in war making. [6]

For such reform to succeed, it must leverage the most significant weapon in Congress's arsenal: the ***power*** of the purse. [7] Because Congress can no longer control the use of military force by declining to declare war, the appropriations ***power*** is likely Congress's strongest tool to influence ***national security*** decision making. However, the ***power*** of the purse is not functioning as the strong check the Framers envisioned. This Note explores a new tool that Congress can use to **[*2516]** reassert its constitutional role in the conduct of war, and in ***national security*** more generally: Appropriations Clause litigation.

While focused on issues of ***national security*** and foreign affairs, this Note also considers the benefits of Appropriations Clause litigation for the separation of ***powers*** generally. The ***power*** of the purse is one of Congress's core checks on the ***executive*** branch, but it is not used as often or as effectively as it could be. [8] The threat of litigation is an important way to give the appropriations ***power*** more bite. And in doing so, it could reduce interbranch friction regarding the branches' respective roles in ***national security***, since the appropriations dispute acts as a proxy for deeper interbranch disagreements. [9] The clarity that the

---

[2] *See* LOUIS FISHER, PRESIDENTIAL WAR ***POWER***, at xiv (3d ed. 2013) ("President Bill Clinton used military force repeatedly without ever seeking authority from Congress, intervening in Iraq, Somalia, Haiti, Bosnia, Sudan, Afghanistan, and Yugoslavia.").

[3] Bruce Ackerman & Oona Hathaway, *Limited War and the Constitution: Iraq and the Crisis of Presidential Legality*, 109 MICH. L. REV. 447, 495-96 (2011).

[4] *See* FISHER, *supra* note 2, at 291 ("The drift of the war ***power*** from Congress to the President after World War II is unmistakable . . . . That is not the framers' model.").

[5] HAROLD HONGJU KOH, THE ***NATIONAL SECURITY*** CONSTITUTION: SHARING ***POWER*** AFTER THE IRAN-CONTRA AFFAIR 38 (1990) ("Even a glimpse of recent history [in ***national security*** affairs] reveals a consistent pattern of ***executive*** circumvention of legislative constraint in foreign affairs that stretches back to the Vietnam War and persists after the Iran-contra affair.").

[6] Ackerman & Hathaway, *supra* note 3, at 458.

[7] *See* Reid Skibell, *Separation of* ***Powers*** *and the Commander-in-Chief: Congress's Authority To Override Presidential Decisions in Crisis Situations*, 13 GEO. MASON L. REV. 183, 195 (2004) ("[T]he spending ***power*** has become Congress's primary tool in influencing military and, to a large degree, foreign policy decisions."); *see also* FISHER, *supra* note 2, at 298 ("Congressional (and public) control would be greatly strengthened if tied to the ***power*** of the purse.").

[8] JOSH CHAFETZ, CONGRESS'S CONSTITUTION: LEGISLATIVE AUTHORITY AND THE SEPARATION OF ***POWERS*** 3, 45 (2017).

[9] This Note focuses on Congress's role vis-à-vis the ***Executive*** in appropriating for and shaping "***national security***" as a whole. I treat war ***powers***, and the constitutional conflict about the proper role of the political branches in war making, as a subset of "***national security***." This broader category also includes issues pertaining to domestic security, terrorism, and foreign relations, among others. Notwithstanding my broader focus, I often specifically invoke war

Appropriations Clause provides could also bring some stability to courts' inconsistent separation-of-***powers*** jurisprudence. [10] Even if the litigation does not succeed, legislators' collective decision to sue can signal to their most important audiences--the President, agencies, the courts, and the public--that Congress is serious about protecting both its policy priorities and its ***power*** over the federal treasury.

Part I examines the appropriations ***power***, its ***original*** understanding, and modern issues with its application. Part II asks whether ***national security*** appropriations litigation is a desirable innovation, concluding that it could help Congress reassert its role vis-à-vis the ***Executive*** in funding ***national security*** and war making. Part III assesses the doctrinal possibility and political feasibility of Appropriations Clause litigation as a congressional tool. Part IV examines the mechanics of an Appropriations Clause lawsuit in the ***national security*** context, addressing the major hurdles to the success of such litigation. This Part then ties these hurdles back to the Supreme Court's adoption, during and after the Vietnam War, of a restrictive and waning view of its own role in separation-of-***powers*** disputes. Part V explores the benefits that Appropriations Clause litigation can provide Congress, in terms of both intra- and interbranch relations, even if the litigation does not succeed. Part VI addresses possible critiques of the ***national security*** Appropriations Clause litigation strategy. Finally, this Note **[*2517]** concludes that appropriations-focused ***national security*** litigation could succeed in the courts, and in doing so could aid Congress in reclaiming its constitutional role, thereby resetting the balance of ***power***.

I. THE MODERN IMBALANCE IN *NATIONAL SECURITY POWERS* AND THE WEAKENED *POWER* OF THE PURSE

The ***power*** of the purse, as ***originally*** understood and applied, served as a real check on the President's ***national security*** activities. As Ackerman and Hathaway observe, the ***power*** of the purse was "once a highly effective mechanism for forcing the president to operate within congressional limits." [11] However, "Congress has failed to adapt this ***power*** to meet modern challenges," [12] and as a result the purse strings are no longer as effective as they once were.

The declining ***power*** of the appropriations ***power*** is attributable to shifts in both budget practice and the political environment. The modern structure of ***national security*** funding--consisting of lump-sum appropriations, as well as flexible tools like transfer and reprogramming authority (discussed below)--gives the President significant discretion in how military funds are spent. As a result, when Congress wants to exercise its appropriations ***power*** in this context, it faces an "uphill battle" [13] and must often resort to concessions and compromise. [14] This Part examines the early history of Congress's appropriations ***power*** in ***national security***, the modern state of this ***power***, and failed attempts to resurrect Congress's waning role. In light of history, modern practice, and failed attempts at reform, Appropriations Clause litigation provides a new tactic that could help resurrect Congress's appropriations ***power*** in the ***national security*** context.

---

powers in this Note because they provide sharp examples of conflicts between Congress and the ***Executive*** in the ***national security*** arena, which are often played out through disputes over appropriations.

[10] On the courts' inconsistency, see, for example, M. Elizabeth Magill, *Beyond **Powers** and Branches in Separation of **Powers** Law*, 150 U. PA. L. REV. 603, 609-10 (2001).

[11] Ackerman & Hathaway, *supra* note 3, at 450.

[12] *Id.*

[13] *Id.* at 486.

[14] *See* KOH, *supra* note 5, at 133.

A. The Evolution of the Appropriations Clause: From the Framing to the Present

The appropriations ***power*** is not what it once was. Congress effectively managed the ***national security*** purse strings in the early days of the Republic, just as the Constitution intended. The Framers envisioned the ***power*** of the purse as "the most complete and effectual weapon with which any constitution can arm the immediate representatives of the people, for obtaining a redress of every **[*2518]** grievance, and for carrying into effect every just and salutary measure." [15] The ***power*** of the purse had great import in the ***national security*** context, conceived as the best means to "prevent the ***executive*** from misusing the sword." [16] Confirming this view, Thomas Jefferson famously wrote: "We have already given . . . one effectual check to the Dog of war by transferring the ***power*** of letting him loose from the ***Executive*** to the Legislative body, from those who are to spend to those who are to pay." [17]

To effectuate the use of the purse strings as a check on the ***Executive***, early appropriations were specific and narrow. Consequently, "they gave Congress significant control over military action. Indeed, a single chamber of Congress could then prevent the initiation or continuation of a military conflict by refusing to fund the war." [18] For example, during the first major military action under the Constitution--a conflict between the militia and Indian tribes from 1789-91--Congress exercised very strict control via appropriations, specifically appropriating "everything from the precise numbers of troops to their al[l]otted daily rations" [19] and salaries. [20] Each time President Washington sought to launch a new campaign or raise more troops for the effort, he had to return to Congress for authorization and appropriations. [21]

If a true emergency arose for which there were no appropriations, the practice that developed early in American history was for Presidents to act first and then seek an ex post, retroactive appropriation from Congress as soon as possible. [22] Congress would then have the option of approving the appropriation

---

[15] THE FEDERALIST NO. 58, at 357 (James Madison) (Clinton Rossiter ed., 2003); *see*WILLIAMC. BANKS & PETER RAVEN-HANSEN, ***NATIONAL SECURITY*** LAW AND THE ***POWER*** OF THE PURSE 172 (1994) (noting that there was "no dissent to Madison's characterization of the appropriation ***power*** . . . and repeated affirmation during the ratification debates that this ***power*** had particular force in ***national security***").

[16] BANKS & RAVEN-HANSEN, *supra* note 15, at 30; *see also id.* at 27 (noting a "widely shared assumption" among the Framers "that the people could risk vesting war ***powers*** and the command of a standing army in the president because Congress retained control of the means of war").

[17] Letter from Thomas Jefferson to James Madison (Sept. 6, 1789), *in* 15 THE PAPERS OF THOMAS JEFFERSON 392, 397 (Julian P. Boyd ed., 1958) (footnote omitted).

[18] Ackerman & Hathaway, *supra* note 3, at 477.

[19] *Id.* at 478.

[20] *Id.* at 480.

[21] *Id.* at 480-81.

[22] *See* BANKS & RAVEN-HANSEN, *supra* note 15, at 37-38; FISHER, *supra* note 2, at 293; LUCIUS WILMERDING, JR., THE SPENDING ***POWER***: A HISTORY OF THE EFFORTS OF CONGRESS TO CONTROL EXPENDITURES 19 (1943) ("The high officers of the government, and a fortiori the President, have a right, indeed a duty, to do what they conceive to be indispensably necessary for the public good, provided always that they submit their action to Congress to sanction the proceeding."). *But see* NLRB v. Noel Canning, 134 S. Ct. 2550, 2610 (2014) (Scalia, J., concurring) ("[A] natural disaster might occur to which the ***Executive*** cannot respond effectively without a supplemental

or **[*2519]** subjecting the President to political retribution if it deemed the expenditure unnecessary. [23] Throughout American history, Presidents have followed this practice of spending unauthorized funds and seeking ex post congressional appropriations as soon as possible. [24]

Early practice around ***national security*** appropriations thus displayed a reciprocal dynamic. Congress appropriated narrowly to exert control over war making. And even where the President withdrew unappropriated funds, he invariably sought ex post authorization from Congress and risked the mantle of unconstitutional action if Congress refused to appropriate the funds.

Modern appropriations, however, are no longer so narrow and specific. The President no longer needs to seek congressional appropriations before launching a military campaign, and Presidents have sufficient contingency and transferable funds already appropriated to respond to any emergency. [25] Congress's modern implementation of the Appropriations Clause in general has been a history of "efforts to assert legislative control over government spending" that have "not always been thorough and consistent." [26]

Today, ***national security*** appropriations take the form of "lump sums for broad categories." [27] The Armed Services Committee reaches these lump-sum figures by adding up lists of itemized expenditures for specific objects, but those **[*2520]** itemizations are not legally binding. [28] These broad appropriations "giv[e] the [P]resident immense discretion to reallocate funds from one activity to another." [29] Beyond the discretion to spend within the broad categories, the use of contingency funds and emergency spending, as well as of reprogramming and transfer authority, has given the ***Executive*** broad modern ***power*** over how appropriations are used. [30]

---

appropriation. But in those circumstances, the Constitution would not permit the President to appropriate funds himself. *See* Art. I, § 9, cl. 7.").

[23] *See* Kate Stith, *Congress' **Power** of the Purse*, 97 YALE L.J. 1343, 1351-52 (1988).

[24] *See also* Gerhard Caspar, *Appropriations of **Power***, 13 U. ARK. L. REV. 1, 20 (1990) (noting that even Robert Gallatin, the first major opponent of lump sum ***national security*** appropriations, acknowledged that the Secretary of War could spend beyond the contingency appropriations in the event of "pressing necessity"). For example, after the British attacked an American frigate in 1807, President Jefferson authorized spending for military provisions in the absence of an appropriation from Congress, and asked Congress when it next convened for an appropriation to cover the expenditures. *See id.* at 21-22. Similarly, President Lincoln directed the Secretary of the Treasury to withdraw two million dollars in unappropriated funds for requisitions to prepare the military and the navy in advance of the Civil War. *See* WILMERDING, *supra* note 22, at 14. And President Grant used up all regular appropriations to put the navy on "war footing" in preparation for war with Spain, which Congress subsequently approved and appropriated four million dollars to cover. *Id.* at 16.

[25] Ackerman & Hathaway, *supra* note 3, at 482 ("As the federal government became more complex and extensive, Congress gradually gave up the detailed budgetary oversight that it held at the Founding.").

[26] Stith, *supra* note 23, at 1396.

[27] BANKS & RAVEN-HANSEN, *supra* note 15, at 50.

[28] *Id.*

[29] Ackerman & Hathaway, *supra* note 3, at 491.

[30] BANKS & RAVEN-HANSEN, *supra* note 15, at 175. Notably, emergency spending was used to initially finance Operation Desert Shield. *Id.* at 72.

Reprogramming funds within a particular account may require "reporting to and sometimes prior approval by [congressional] committees" depending on the amount to be reprogrammed and the object, but "[t]he thresholds do permit considerable reprogramming without committee knowledge." [31] Reprogrammed funds are often used to carry out unfunded ***national security*** objectives. [32] For example, the relevant oversight committee approved reprogramming of appropriations between missions to fund the operation that culminated in the Bin Laden raid. [33] And reprogrammed funds "were used to station troops in Honduras [in the 1980s] and to construct permanent bases there without authorization for military construction," for the benefit of the Contras. [34]

Transfer authority--the ability to move funds between appropriations accounts--is another source of ***executive*** discretion that blunts the force of the appropriations ***power***. The Department of Defense (DOD) is given transfer authority in its annual appropriations act, and "transfer authority abuses are fairly common." [35] The President can also transfer funds among agencies under the **[*2521]** Economy Act of 1932. [36] The President has used transfers to circumvent congressional limits on funding in the past. For instance, President Nixon used DOD transfers to continue bombing Cambodia after the withdrawal of troops from Vietnam; and, after the Boland Amendment prohibited funding the Contras, President Reagan transferred equipment from DOD to the CIA to give to the Contras anyway. [37] Broad appropriations categories, combined with expansive authority to transfer and reprogram funds between programs, mean that Congress is effectively excised from influencing *how* ***national security*** funds are spent.

The recent intervention in Libya typifies how the appropriations ***power*** has left Congress unable to check zealous presidential intervention. In that case, President Obama initiated military operations without congressional authorization or appropriations. Although the House voted overwhelmingly against supporting the mission, it was unable to muster a successful vote to cut off funding. [38] This situation demonstrates the modern difficulties preventing Congress from effectively exercising its ***power*** of the purse in ***national security***. First, broad defense appropriations "allowed Administrations to deploy forces into

---

[31] *Id.* at 76.

[32] For example, President Reagan "routinely used the reprogramming authority to fund Central American projects that Congress had not approved." KOH, *supra* note 5, at 131.

[33] Greg Miller, *CIA Spied on bin Laden from Safe House*,WASH. POST (May 6, 2011), http://www.washingtonpost.com/world/cia-spied-on-bin-laden-from-safe-house/2011/05/05/AFXbG31F_story.html [http://perma.cc/ZUW7-54RD]. While notification and reprogramming approval may appear to be a partial congressional check on ***national security*** appropriations, these do not compensate for loss of the ***power*** of the purse as a check. For example, only the relevant oversight committee must approve the reprogramming, and there is potential for committee capture and easy acquiescence.*Cf.* Heidi Kitrosser, *Congressional Oversight of* ***National Security*** *Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1079 (2008) (discussing the complexities of involving multiple committees in ***national security*** matters).

[34] BANKS & RAVEN-HANSEN, *supra* note 15, at 77.

[35] *Id.*

[36] *Id.* at 78.

[37] *Id.*

[38] *See* Jennifer Steinhauer, *House Spurns Obama on Libya, but Does Not Cut Funds*, N.Y. TIMES (June 24, 2011), http://www.nytimes.com/2011/06/25/us/politics/25powers.html [http://perma.cc/79W4-3CGM].

regions of potential conflict without advance funding approval from Congress." [39] Indeed, President Obama funded the entire operation in Libya out of existing appropriations, without requiring a new appropriation from Congress. [40] In this scenario, congressional inaction is not sufficient to prevent military intervention; [41] contrary to the Framers' plan, a majority of one house is no longer sufficient to prevent funding an operation. [42] A majority of the House questioned the **[*2522]** President's initiation of operations without authorization, and refused to authorize the action in Libya. [43] Their opposition would have been enough to prevent the operation in the system designed by the Framers, but it was insufficient in our modern system where the burdens have been redistributed.

Congress could still have prohibited the expenditure of appropriations for combat activities in Libya, but opponents were not able to get support for this measure, [44] as the political pressures on Congress to support military operations in progress made such a prohibition functionally impossible. [45] Members of Congress are often unwilling to pay the "high . . . political price" of being "accused of abandoning the troops in the field." [46] Even if Congress were willing to risk political suicide, it would need two-thirds of each house to pass a funding restriction over a President's veto. [47] The difficulty of meeting this threshold puts the

---

[39] Ackerman & Hathaway, *supra* note 3, at 477 (quoting STEPHEN DAGGETT, CONG. RESEARCH SERV., MEMORANDUM: BUDGETING FOR WARS IN THE PAST 1 n.1 (Mar. 27, 2003)).

[40] *Cf.* BANKS & RAVEN-HANSEN, *supra* note 15, at 180 (noting that Presidents have a "rich menu of discretionary spending authorities" and "[b]y picking from this menu presidents have successfully stretched the law instead of breaking it").

[41] John C. Yoo, *The Continuation of Politics by Other Means: The **Original** Understanding of War **Powers***, 84 CALIF. L. REV. 167, 297 (1996).

[42] *See* Louis Fisher, *Historical Survey of the War **Powers** and the Use of Force, in* THE U.S. CONSTITUTION AND THE ***POWER*** TO GO TO WAR: HISTORICAL AND CURRENT PERSPECTIVES 11, 23-24 (Gary M. Stern & Morton H. Halperin eds., 1994) (noting that the "congressional ***power*** of the purse" is "most potent when the President is seeking funds . . . . But when Congress is attempting to use an appropriations bill to terminate funding, the President may veto that bill and force Congress to locate a two-thirds majority in each House for an override").

[43] *See* Steinhauer, *supra* note 38.

[44] *Id.*

[45] Note, *Recapturing the War **Power***, 119 HARV. L. REV. 1815, 1831 (2006); *see also* Jack Goldsmith, *The Potential Relevance of OLC's Kosovo-War **Powers** Resolution Opinion to the Syria Debate*, LAW-FARE (Sept. 2, 2013, 9:33 AM), http://www.lawfareblog.com/potential-relevance-olcs-kosovo-war-***powers***-resolution-opinion-syria-debate [http://perma.cc/4YXG-ZYGU] (explaining that "declining appropriations could be viewed as 'not supporting the troops in battle'").

[46] Ackerman & Hathaway, *supra* note 3, at 450; *see* Yoo, *supra* note 41, at 298 (noting that during the Bosnian operation, the House failed to cut funding and ultimately "passed a resolution opposing President Clinton's policy, but supporting the troops").

[47] *See* Ackerman & Hathaway, *supra* note 3, at 486 (discussing the "uphill battle" of overcoming the veto); *see also id.* at 490 (discussing President Clinton's threats to veto congressional funding cut-offs regarding the Kosovo operation).

President in a strong bargaining position, enabling her to extract concessions and compromises and to weaken even the modest funding restrictions Congress tries to impose. [48]

Overall, the ***power*** of the purse has transformed from a robust ex ante legal check on unilateral ***executive*** action to a hobbled ex post political tool. Congress may influence war making more informally, through political pressure, [49] but it is unable to use its constitutional ***power*** to keep chained or completely recall the **[*2523]** dog of war. [50] As Douglas Kriner has written, "in almost every case of interbranch conflict over military policy, the ***power*** of the purse has proven to be a blunt instrument whose costs, both strategic and political, have virtually precluded its successful use." [51] This is a far cry from the constitutional distribution of war ***powers*** that the Framers envisioned and employed.

B. Failed Attempts To Correct the Imbalance Through Congressional Litigation

Congress has occasionally sought to reassert its proper role. However, attempts to correct this imbalance over the past forty years have been unsuccessful. The adoption of the War ***Powers*** Resolution (WPR) failed to revive Congress's constitutional role in war making. [52] Alternatively, individual members of Congress have sought to vindicate Congress's role in ***national security*** by seeking judicial redress in specific disputes with the ***Executive***. [53] The rejection of these lawsuits demonstrates that judicial redress--in the forms sought by members of Congress thus far--has been insufficient to correct the imbalance in the separation of ***powers***. However, it demonstrates that members of Congress *are* eager to seek judicial redress. Appropriations Clause litigation presents a new strategy that legislators could use to reassert their constitutional prerogative.

*1. War **Powers** Litigation*

"The phenomenon of litigation directly between Congress and the President concerning their respective constitutional ***powers*** . . . is a recent one." [54] The first such lawsuit was a challenge to the Vietnam War, brought in 1972. [55] Members of Congress have since brought twelve separate lawsuits, claiming that the President **[*2524]** unconstitutionally exercised war ***powers*** without congressional authorization. None

---

[48] *See supra* note 14 and accompanying text; *see also* KOH, *supra* note 5, at 133 ("Even when Congress has successfully forced the president to the bargaining table . . . the president has usually been able to demand concessions or future support in exchange for agreeing to modify his conduct.").

[49] KRINER, *supra* note 1, at 148-51 (discussing congressional opposition during the Iraq war).

[50] *See id.* at 148 ("[I]n none of the 122 major uses of force analyzed . . . [by Kriner] did Congress successfully exercise its ***power*** of the purse or the War ***Powers*** Resolution to compel the president to end a military engagement against his will.").

[51] *Id.* at 41.

[52] *See* WILLIAM G. HOWELL & JON C. PEVEHOUSE, WHILE DANGERS GATHER: CONGRESSIONAL CHECKS ON PRESIDENTIAL WAR ***POWERS*** 4-5 (2007).

[53] *See* Carlin Meyer, *Imbalance of **Powers**: Can Congressional Lawsuits Serve as Counterweight*?, 54 U. PITT. L. REV. 63, 106 n.209 (1992).

[54] Id. at 73 (quoting Barnes v. Kline, 759 F.2d 21, 41 (D.C. Cir. 1984) (Bork, J., dissenting), *vacated as moot sub nom*. Burke v. Barnes, 479 U.S. 361 (1987)).

[55] Gravel v. Laird, 347 F. Supp. 7 (D.D.C. 1972); *see* Meyer, *supra* note 53, at 73.

have reached the merits. [56] Courts have dismissed these lawsuits on various procedural grounds: the political-question doctrine, [57] equitable discretion, [58] ripeness, [59] standing, [60] and mootness. [61]

The most recent of these suits, *Kucinich v. Obama*, provides a good example of the judicial barriers to congressional war ***powers*** litigation. In *Kucinich*, ten members of the House sued President Obama, arguing that the President's military involvement in Libya without authorization from Congress violated both **[*2525]** the War ***Powers*** Clause of the Constitution and the WPR. [62] The plaintiffs asked the court to declare that the "military operations in Libya constitute[d] a war for the purposes of Article I" and were therefore "unconstitutional absent a declaration of war from Congress." [63] The legislators further requested that the court declare "unconstitutional the policy of the Administration that the President may use previously appropriated funds to support 'an undeclared war,'" and asked for an injunction "suspending all U.S. military operations in Libya absent a declaration of war from Congress." [64] The district court dismissed the case,

---

[56] FISHER, *supra* note 2, at 302 ("In recent decades, federal courts have consistently refused to reach the merits in war ***power*** cases.").

[57] *See* Sanchez-Espinoza v. Reagan, 770 F.2d 202 (D.C. Cir. 1985) (dismissing a lawsuit by twelve members of the House of Representatives who challenged the aid given to Nicaraguan Contras); Crockett v. Reagan, 720 F.2d 1355 (D.C. Cir. 1983) (per curiam) (dismissing a lawsuit by twenty-nine members of Congress who challenged military assistance to El Salvador as violation of war ***powers***); Mitchell v. Laird, 488 F.2d 611 (D.C. Cir. 1973) (dismissing a lawsuit by thirteen members of the House of Representatives who challenged the Vietnam War); Holtzman v. Schlesinger, 484 F.2d 1307 (2d Cir. 1973) (dismissing a lawsuit by a member of Congress who challenged bombings in Cambodia); Drinan v. Nixon, 364 F. Supp. 854 (D. Mass. 1973) (dismissing a lawsuit by four members of the House of Representatives who challenged the bombings in Cambodia); Gravel, 347 F. Supp. 7 (dismissing a lawsuit by two senators and twenty members of the House of Representatives who challenged the constitutionality of the Vietnam War).

[58] *See* Crockett, 720 F.2d 1355; Lowry v. Reagan, 676 F. Supp. 333 (D.D.C. 1987) (dismissing a lawsuit in which 110 members of the House of Representatives argued that the President was required to file a WPR report following military actions in the Persian Gulf); Conyers v. Reagan, 578 F. Supp. 324 (D.D.C. 1984) (dismissing a lawsuit by eleven members of the House of Representatives who challenged the military invasion of Grenada).

[59] *See* Doe v. Bush, 323 F.3d 133, 134 (1st Cir. 2003) (dismissing a lawsuit brought by twelve members of the House, among others, to prevent the President from initiating war with Iraq due to a lack of ripeness); Dellums v. Bush, 752 F. Supp. 1141, 1149-52 (D.D.C. 1990) (denying a preliminary injunction sought by fifty-four members of Congress to prevent the President's impending attack on Iraq).

[60] *See* Campbell v. Clinton, 203 F.3d 19, 20 (D.C. Cir. 2000) (dismissing, for lack of standing, a lawsuit brought by thirty-one members of Congress arguing that the U.S. involvement in the Kosovo intervention violated the War ***Powers*** Clause and WPR); Holtzman, 484 F.2d at 1315 (giving instructions to the district court to dismiss a lawsuit brought by a member of the House and others to stop the U.S. bombing of Cambodia for lack of standing, among other reasons); Kucinich v. Obama, 821 F. Supp. 2d 110, 112 (D.D.C. 2011) (holding that ten members of the House did not have standing to argue that the President's military involvement in Libya violated the War ***Powers*** Clause); Gravel, 347 F. Supp. at 9 (dismissing a lawsuit brought by over twenty members of Congress seeking to stop the Vietnam war for lack of standing).

[61] *See* Conyers v. Reagan, 765 F.2d 1124, 1129 (D.C. Cir. 1985) (dismissing an appeal brought by members of Congress surrounding their lawsuit to stop the invasion of Grenada as moot). reviving the ***power*** of the purse

[62] Kucinich, 821 F. Supp. 2d at 112-13.

[63] Id. at 113.

[64] Id. at 114.

holding that the plaintiffs did not fit into the "very limited circumstances in which a member of Congress might successfully assert legislative standing." [65] *Kucinich* is a prime example of a pervasive trend in congressional litigation: courts are eager to do anything in their ***power*** to prevent such suits from reaching the merits. But courts have eagerly blocked congressional lawsuits against the president in other contexts, as well--as we will see.

2. ***National Security*** *Litigation: Intelligence and Funding*

Congressional plaintiffs have also brought lawsuits against the ***Executive*** that did not involve war ***powers***. Although the constitutional imbalance between the President and Congress is most glaring in the war-***powers*** context, it also affects ***national security*** policy more generally. Members of Congress have occasionally sought to address that imbalance through litigation.

Congressional plaintiffs have brought a number of lawsuits against the ***Executive*** touching upon ***national security***, intelligence, and disclosure. In a FOIA challenge involving top-secret nuclear test information, congressional plaintiffs lost on the merits. [66] In two challenges to the legality of intelligence activity, [67] and in a challenge to ***executive*** nondisclosure agreements that prevented federal **[*2526]** employees from communicating secret information to Congress, [68] the court found that congressional plaintiffs lacked standing. [69]

Another set of lawsuits brought by congressional plaintiffs against the ***Executive*** falls under the general category of ***national security*** funding. Four of these lawsuits were dismissed for lack of standing. [70] In

---

[65] Id. at 116.

[66] *See* EPA v. Mink, 410 U.S. 73 (1973) (denying an attempt by members of Congress to force the government to produce top-secret information about an underground nuclear test under FOIA).

[67] *See* United Presbyterian Church in the U.S.A. v. Reagan, 738 F.2d 1375, 1382 (D.C. Cir. 1984) (finding lack of standing where a member of Congress and others challenged the legality of ***Executive*** Order No. 12333, which established an intelligence gathering framework); Harrington v. Bush, 553 F.2d 190, 199 (D.C. Cir. 1977) (finding that a member of the House lacked standing in a lawsuit to enjoin the CIA from engaging in illegal activities).

[68] Nat'l Fed'n of Fed. Emps. v. United States, 688 F. Supp. 671, 679-80 (D.D.C. 1988) (finding that seven members of Congress lacked standing to sue to enforce an appropriations restriction prohibiting the President from using federal employee nondisclosure agreements to prevent Congress from receiving classified information), *vacated sub nom*. Am. Foreign Serv. Ass'n v. Garfinkel, 490 U.S. 153 (1989).

[69] For example, in *United Presbyterian Church in the U.S.A. v. Reagan*, the D.C. Circuit held that a congressman's argument that his "***powers*** as a legislator have been diminished" by the illegality of an ***executive*** order constituted a "generalized grievance." 738 F.2d at 1381-82.

[70] *See* Harrington, 553 F.2d at 199 (finding that a member of the House lacked standing in a lawsuit to enjoin the CIA from engaging in illegal activities); Harrington v. Schlesinger, 528 F.2d 455, 456 (4th Cir. 1975) (dismissing, for lack of standing, a lawsuit brought by four members of Congress alleging that the U.S. involvement in Vietnam after 1973 violated two appropriations restrictions and the Appropriations Clause); Spence v. Clinton, 942 F. Supp. 32, 36-38 (D.D.C. 1996) (finding that forty-one members of Congress did not have standing at the time of the case to argue that the President violated the Ballistic Missile Defense Act and refused to spend funds on a specific missile system in violation of the Defense Appropriations Act); *Nat'l* Fed'n of Fed. Emps., 688 F. Supp. at 679-80 (finding that seven members of Congress lacked standing to sue to enforce an appropriations restriction prohibiting the President from using federal employee nondisclosure agreements to prevent Congress from receiving classified information, though the court ultimately ruled the restriction unconstitutional).

addition, one war-***powers*** lawsuit involved a claim that the President violated explicit appropriations restrictions against aiding the Nicaraguan Contras, but this claim was dismissed as moot because the annual appropriations act involved had lapsed. [71] Significantly, it appears that only one ***national security*** challenge brought by a congressional plaintiff was raised directly under the Appropriations Clause. This was *Harrington v. Schlesinger*, in which four members of Congress alleged that U.S. involvement in Vietnam after 1973 violated two explicit appropriations restrictions and the Appropriations Clause. [72] The Fourth Circuit held that the congressmen could not "claim dilution of their legislative voting ***power*** because the legislation they favored became law," and therefore they did not have standing. [73] The court reasoned that the congressmen could seek "legislative resolution" of their claims, and implied that the fact "that the Congress has done nothing suggests that the ***Executive***'s interpretation of the statutes is in agreement with the **[*2527]** congressional intent." [74] As will be discussed later, these standing and acquiescence arguments are among the more common barriers to judicial review of ***national security*** issues, but a determined Congress or congressional chamber can surmount them.

Congressional plaintiffs have also brought a number of challenges against ***executive*** treaty-making activities. These have been squarely rejected for presenting nonjusticiable political questions [75] or for lack of standing. [76] Similarly, congressional plaintiffs have brought a number of challenges to ***executive*** actions regarding foreign aid. These have been dismissed under equitable discretion doctrine, [77] for lack of standing, [78] for presenting a nonjusticiable political question, [79] or for mootness. [80]

---

[71] Sanchez-Espinoza v. Reagan, 770 F.2d 202, 210 (D.C. Cir. 1985) (dismissing as moot a claim by twelve members of the House challenging U.S. aid to Nicaraguan contras).

[72] 528 F.2d at 456.

[73] Id. at 459.

[74] *Id.*

[75] *See* Dole v. Carter, 569 F.2d 1109, 1110 (10th Cir. 1977) (rejecting a senator's challenge to the President's unilateral attempt to return a World War II relic to Hungary as a treaty requiring the advice and consent of the Senate); Kucinich v. Bush, 236 F. Supp. 2d 1, 14-18 (D.D.C. 2002) (dismissing an action brought by thirty-two members of the House challenging the unilateral withdrawal from the 1972 Anti-Ballistic Missile Treaty); Cranston v. Reagan, 611 F. Supp. 247, 254 (D.D.C. 1985) (finding nonjusticiable the claim by three members of Congress who argued that the nuclear treaty with Sweden violated the Atomic Energy Act).

[76] Kucinich, 236 F. Supp. 2d at 4-12.

[77] Dornan v. U.S. Sec'y of Def., 851 F.2d 450, 451 (D.C. Cir. 1988) (rejecting the claim of sixteen members of Congress who sought to prevent the ***Executive*** from complying with Boland amendments); Helms v. Sec'y of the Treasury, 721 F. Supp. 1354, 1359 (D.D.C. 1989) (rejecting the claims of six members of Congress who sought to challenge the ***Executive***'s inclusion of Namibia as a target for anti-apartheid sanctions).

[78] Dornan, 851 F.2d at 451; Burton v. Baker, 723 F. Supp. 1550, 1554 (D.D.C. 1989) (holding that four House members had no standing when they challenged a "side agreement" between the ***Executive*** and legislative leadership regarding appropriated funds to be spent in humanitarian aid to Nicaragua).

[79] Burton, 723 F. Supp. at 1554.

[80] Burke v. Barnes, 479 U.S. 361, 362-63 (1987) (rejecting as moot a challenge by thirty-three House members, with the Senate and Bipartisan Leadership Group of the House as intervenors, to the President's pocket veto of bill regarding military aid to El Salvador).

The prevalence of these lawsuits demonstrates that congressional plaintiffs seek to vindicate Congress's constitutional role in ***national security***, beyond the most visible conflicts regarding war ***powers***. Although no case has succeeded on the merits, such lawsuits may serve as useful prequels to an Appropriations Clause challenge. As the foregoing Section demonstrates, the range of ***national security*** issues that Appropriations Clause lawsuits could affect is much broader than the core war-making ***power***. Indeed, an Appropriations Clause suit could be deployed in a variety of contexts that reflects the many ways in which the President wields disproportionate weight in the military arena.

[*2528] I I . THE NORMATIVE CASE FOR CONGRESS LITIGATING ITS PURSE STRINGS

Thus far, legislative reform and attempts to appeal to the judiciary have not succeeded in correcting the constitutional ***national security*** imbalance. An Appropriations Clause case could more effectively vindicate the vision that the Framers intended and prevent the accretion of disproportionate ***power*** to the ***Executive***. Such a suit would proceed in two steps. First, Congress would appropriate funding for ***national security***, either attaching an explicit restriction stating that no funds are being appropriated for purpose *x*, or appropriating in narrow categories such as to make clear through its omission that purpose *x* has not been funded. Then, when the ***Executive*** pursues *x* by withdrawing and spending funds that have been appropriated for another activity, Congress--or one chamber thereof--would pass a resolution to bring a lawsuit against the ***Executive*** for violating the Appropriations Clause. Specifically, the lawsuit would allege that the President violated the Constitution by "draw[ing]" money "from the Treasury" not "in Consequence of Appropriations made by Law." [81] Congressional Appropriations Clause litigation has the opportunity to serve as a beneficial tool for reinforcing the appropriations ***power*** in ***national security***. The use--or merely the threatened use--of these lawsuits could revive Congress's biggest check on ***Executive*** war making and increase Congress's political bargaining ***power*** in ***national security*** policy making.

Appropriations litigation, first and foremost, can help reassert Congress's constitutional role in ***national security*** disputes. "The multiple constitutional prerequisites for government activity"--such as the necessity of congressional appropriation before undertaking an action--"are checks upon the exercise of government ***power***, reflecting the foundational decision that the exercise of such ***power*** should be deliberate and limited." [82] Though modern presidential spending discretion in ***national security*** means that appropriations are no longer prerequisites for a specific activity, judicial review can reinvigorate appropriations as an ex post check on ***executive*** overreach. As both Founding-era thinking and early practice indicate, such a check would create political and legal accountability that is currently lacking in ***national security*** policy making. [83]

The Supreme Court recently reiterated in *Zivotofsky ex rel. Zivotofsky v. Kerry* that "many decisions affecting foreign relations"--including the appropriations **[*2529]** required to carry out those decisions--"require congressional action." [84] Repudiating the broad delegation of ***power*** to the ***Executive*** articulated in *United States v. Curtiss-Wright Export Corp.*, [85] the majority clarified that "[t]he ***Executive*** is not free from the ordinary controls and checks of Congress merely because foreign affairs are at issue." [86] The

---

[81] U.S. CONST. art. I, § 9, cl. 7.

[82] Stith, *supra* note 23, at 1347.

[83] *See supra* notes 15-24 and accompanying text.

[84] 135 S. Ct. 2076, 2087 (2015).

[85] 299 U.S. 304 (1936).

[86] Zivotofsky, 135 S. Ct. at 2090.

dissenting Justices went even further in their defense of Congress's role in the separation of ***powers***. [87] For these sentiments to have any effect, the President must be made to abide by Congress's appropriations decisions. After all, as Chief Justice Roberts noted in his *Zivotofsky* dissent, "the President's ***power*** reaches 'its lowest ebb'" under the traditional *Youngstown* framework "when he contravenes the express will of Congress." [88] By enabling Congress to enforce its appropriations ***power***, the courts can help "restore the balance of ***power***" [89] in the ***national security*** context. [90]

Appropriations litigation can also help redistribute the burdens of making war and funding ***national security*** actions, so as to be more faithful to the Constitution. The constitutional text and history suggest that a majority of either house of Congress is sufficient to reject the decision to declare war, [91] or reject an appropriation to fund a war. However, with the President's spending discretion and ability to begin a conflict without congressional authorization, Congress essentially requires a veto-proof two-thirds majority in each house to defund an **[*2530]** unauthorized war. [92] A congressional Appropriations Clause lawsuit--requiring only a majority of one house to authorize suit--vindicates the ***original*** constitutional distribution of burdens and ***power***. The great gulf between the interbranch cooperation prescribed by the Constitution and the current reality of unilateral ***executive*** action in this area means that Appropriations Clause lawsuits would be particularly valuable in ***national security*** and foreign-relations cases.

Furthermore, these lawsuits could also improve the balance of ***power*** among the branches as a general matter. As discussed in Part IV, because Appropriations Clause litigation is based on a provision that is unusually clear by constitutional standards, [93] it could spur targeted judicial involvement in interbranch disputes. It could thereby help defuse conflicts between Congress and the President that might otherwise escalate. The breadth and clarity of the appropriations ***power*** makes it perhaps the most potent of a larger

---

[87] Id. at 2113 (Roberts, C.J., dissenting) ("Today's decision is a first: Never before has this Court accepted a President's direct defiance of an Act of Congress in the field of foreign affairs . . . . I write separately to underscore the stark nature of the Court's error on a basic question of separation of ***powers***."); id. at 2126 (Scalia, J., dissenting) ("International disputes about statehood and territory are neither rare nor obscure . . . . A President empowered to decide all questions relating to these matters, immune from laws embodying congressional disagreement with his position, would have uncontrolled mastery of a vast share of the Nation's foreign affairs.").

[88] Id. at 2113 (Roberts, C.J., dissenting).

[89] Meyer, *supra* note 53, at 106-07 (advocating in favor of expanded congressional standing to help vindicate the separation of ***powers*** generally and "contain [the modern] enhancement of ***executive power*** in areas arguably allocated elsewhere by the Constitution").

[90] Andrew D. LeMar, Note, *War **Powers**: What Are They Good for?: Congressional Disapproval of the President's Military Actions and the Merits of a Congressional Suit Against the President*, 78 IND. L.J. 1045, 1067 (2003) ("Congress must turn to the judiciary in order to regain the war-making ***powers*** that Presidents have taken from it over the past six decades."); *see also* KOH, *supra* note 5, at 223 ("If anything, meaningful judicial review is even more constitutionally necessary in foreign affairs than in domestic affairs.").

[91] U.S.CONST. art. I, § 8, cl. 11 ("The *Congress* shall have ***Power*** . . . [t]o declare War." (emphasis added)).

[92] FISHER, *supra* note 2, at 301 (reasoning that a one-house majority to veto a war "is the correct principle; the requirement of a two-thirds majority in each House [to override a presidential veto] is constitutionally excessive").

[93] *Compare* U.S. CONST. art. I, § 9, cl. 7 ("No money shall be drawn from the treasury, but in consequence of appropriations made by law."), *with* U.S. CONST. art. II, § 2, cl. 1 ("The President shall be Commander in Chief of the Army and Navy of the United States.").

suite of tools with which Congress can exert its authority against the other branches. [94] The clause both vests Congress with the ***power*** to appropriate and "ensur[es] that the money [is] actually spent for the purposes for which it was appropriated." [95] Congress can use this ***power*** generally--depriving the ***executive*** branch of the means to do its work--or specifically--affecting particular policies through riders. [96] Indeed, the Appropriations Clause allows Congress to invade what would otherwise be the President's exclusive ***power*** to execute the law. [97] Instead of asking, in the abstract, whether the ***Executive*** has the authority under the Constitution to engage in a particular activity, a court can focus on the simpler question of whether Congress has appropriated funds for that activity.

To think of this in more familiar terms: if Congress is right in arguing that it has not appropriated funds for the ***Executive***'s actions, or that an appropriations rider prohibits funds from being spent on those actions, then *any* Appropriations **[*2531]** Clause case will be funneled into category three of the tripartite *Youngstown* framework. [98] Because the President's activity is "incompatible with the expressed . . . will of Congress," the President's "***power*** is at its lowest ebb." [99] A congressional decision to sue would throw Congress's disapproval into starker relief, sharpening the conflict and ensuring that appropriations litigation would take place in category three. Under the *Youngstown* framework, the President would only be able to win such a suit if she acts under a ***power*** that is "both 'exclusive' and 'conclusive' on the issue" in dispute--a claim that "must be 'scrutinized with caution.'" [100] And as the Court noted in *Zivotofsky*, even when a President successfully proves that she has exclusive authority over a particular ***power***, Congress can *still* use the Appropriations Clause to shape many of the President's policy decisions under that ***power***. [101] Most cases, therefore, will be rather clear cut: the courts will not need to sift out the two branches' substantive ***powers***, and will be able to rule for Congress on the constitutional question. Appropriations Clause lawsuits, therefore, could simplify and help resolve otherwise intractable separation-of-***powers*** disputes. In the context of this more limited and concrete legal question, the judiciary may be more willing to intervene on Congress's side in constitutional disputes between the political branches.

The possibility of an Appropriations Clause lawsuit is also valuable if the trend of ***executive*** accretion of ***national security power*** at the expense of Congress continues. This kind of lawsuit will become increasingly valuable if the constitutional imbalance in ***power*** increases. Under the current state of our politics, it is not impossible to imagine an imperial unitary ***executive*** with a robust belief in an inherent

---

[94] CHAFETZ, *supra* note 8, at 45.

[95] *Id.* at 56.

[96] *Id.* at 66-67.

[97] *See* John F. Manning, *Separation of* ***Powers*** *as Ordinary Interpretation*, 124 HARV. L. REV. 1939, 1963-64 (2011).

[98] *See* Bob Allen & Sarah Miller, *The Constitutionality of* ***Executive*** *Spending* ***Powers*** 5 (Harvard Law Sch. Fed. Budget Policy Seminar, Briefing Paper No. 38, 2008), http://www.law.harvard.edu/faculty/hjackson/ConstitutionalityOfExecutive_38.pdf [http://perma.cc/T9DM-KVKZ].

[99] Medellin v. Texas, 552 U.S. 491, 525 (2008) (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635, 637-38 (1952) (Jackson, J., concurring)).

[100] Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076, 2084 (2015) (quoting Youngstown, 343 U.S. 638 at 637-38 (Jackson, J., concurring)).

[101] *See id.* at 2087.

executive spending authority winning the presidency and blatantly disregarding Congress's appropriations limits. [102]

Such a President may spend without appropriation in violation of the Constitution if he lacks political hope of persuading Congress to vote in his favor, [103] or is willing to act in the face of potential political retribution. Or he may act **[*2532]** when he mistakenly believes--or wants to believe [104] --that he has the authority to make ***national security*** expenditures without congressional approval. In these circumstances, only adjudication will allow Congress to exercise its appropriations ***power*** to check ***executive*** war making and unilateral ***national security*** policy making.

A robust Appropriations Clause could thus strengthen Congress's constitutional hand in dealing with the ***Executive*** generally. But leaving aside potential benefits for the separation-of-***powers*** jurisprudence, at the very least these lawsuits could help Congress reassert its constitutional role in ***national security***.

III. REASSERTING CONGRESS'S ROLE IN *NATIONAL SECURITY* THROUGH APPROPRIATIONS CLAUSE LITIGATION

This Part examines the feasibility of adjudicating a suit based on the Appropriations Clause, and the possibility of its being invoked by Congress. There have been recent signs that courts are willing to entertain Appropriations Clause suits, and Congress has become active in its attempts to create and enforce funding limits on the President's ***national security*** activities. Both the legal feasibility and the political possibility of a suit are illustrated in the context of a real-life ***national security*** hypothetical: the transfer of detainees from Guantanamo.

A. The (Short) History of Congressional Appropriations Clause Claims

The possibility of a separation-of-***powers*** claim under the Appropriations Clause is not a novel proposition. In the 1970s, individual members of Congress and citizens brought a slew of lawsuits challenging the United States' involvement in the Vietnam War. In one lawsuit, *Harrington v. Schlesinger*, individual legislators and other citizens alleged that President Nixon violated the Appropriations Clause by funding military actions in Vietnam after a statutory funding cut-off date set by Congress. [105] However, the court held that the individual members of Congress and citizens lacked standing to challenge the legality of the ***executive*** actions. [106] After *Harrington*, the Appropriations Clause lay **[*2533]** dormant as a basis for litigation against the ***Executive*** until recently revived by Congress and criminal defendants.

In one recent act of resuscitation, the District Court for the District of Columbia held that a house of Congress could sue the ***Executive*** for violations of the Appropriations Clause. In *U.S. House of Representatives v. Burwell*, the House as an institution sued departments and officials within the ***executive*** branch, alleging that those entities were withdrawing and spending unappropriated funds to pay certain

---

[102] *See generally* J. Gregory Sidak, *The President's* ***Power*** *of the Purse*, 1989 DUKE L.J. 1162 (laying out a theory of the President's implied spending ***power*** in the absence of appropriations).

[103] *See* Ackerman & Hathaway, *supra* note 3, at 508.

[104] *See* Richard D. Rosen, *Funding "Non-Traditional" Military Operations: The Alluring Myth of a Presidential* ***Power*** *of the Purse*, 155MIL. L.REV. 1, 13 (1998) ("To operational lawyers, the proposition that presidential spending authority exists independent of Congress is particularly alluring.").

[105] 528 F.2d 455, 456 (4th Cir. 1975).

[106] Id. at 458-59.

cost-sharing off-sets under the Affordable Care Act (ACA). [107] The district court denied the government's motion to dismiss the Appropriations Clause claim, holding that the House had standing to pursue the claim [108] and that it was justiciable. [109] In May 2016, the district court issued a decision on the merits, holding that the ***executive***-branch agencies and officers had been violating the Appropriations Clause because the ACA did not permanently appropriate the funds at issue. [110] Though *Burwell* was not resolved by the D.C. Circuit because the parties reached a settlement, [111] it is nevertheless significant as the first **[*2534]** Appropriations Clause lawsuit authorized by a body of Congress. [112] Perhaps more importantly, the district court's finding that the legislative plaintiffs were not barred by the various justiciability doctrines hints at a potential shift in the jurisprudential landscape that would allow more legislative suits. Sweeping language in the decision recognized the constitutional significance of the Appropriations Clause

---

[107] 130 F. Supp. 3d 53, 53 (D.D.C. 2015). I served as a lawclerk on the D.C. Circuit while the appeal in this case was pending. I had no involvement in the matter during my clerkship, and the opinions expressed herein are entirely my own.

[108] Id. at 74-75.

[109] Id. at 79-81.

[110] U.S. House of Representatives v. Burwell, 185 F. Supp. 3d 165, 168 (D.D.C. 2016).

[111] The case was held in abeyance with the change of administrations. U.S. House of Representatives v. Hargan, No. 16-5202 (D.C. Cir. Dec. 5, 2016) (holding case in abeyance). In August 2017, the D.C. Circuit allowed seventeen states and the District of Columbia to intervene in defense of the ACA, though the abeyance continued. U.S. House of Representatives v. Hargan, No. 16-5202 (D.C. Cir. Aug. 1, 2017) (granting motion for leave to intervene). In October 2017, the administration officially decided to stop paying the cost-sharing subsidies. Press Release, Dep't Health and Human Serv., Trump Administration Takes Action To Abide by the Law and Constitution, Discontinue CSR Payments (Oct. 12, 2017), http://www.hhs.gov/about/news/2017/10/12/trump-administration-takes-action-abide-law-constitution-discontinue-csr-payments.html [http://perma.cc/3PLZ-VXBF]. In December 2017, the parties informed the D.C. Circuit that they had reached a settlement. U.S. House of Representatives v. Hargan, No. 16-5202 (D.C. Cir. Dec. 15, 2017) (joint report by the parties). And in May 2018, the D.C. Circuit granted the parties' joint motion to dismiss the appeal and remand for the district court to adopt the settlement. U.S. House of Representatives v. Azar, No. 16-5202 (D.C. Cir. May 16, 2018) (dismissal order).

Notably, the settlement agreement asked the district court to vacate its injunction issued on the merits. But it did not ask for vacatur of the decision finding that the House had standing and that the case was justiciable; instead, it merely waived the parties' right to argue that the decision had preclusive effect. U.S. House of Representatives v. Hargan, No. 16-5202 (D.C. Cir. Dec. 15, 2017) (settlement agreement). Thus, even after the settlement, the district court's procedural decision will stand as persuasive precedent in future cases. Moreover, the procedure followed by the House and the district court's opinion provide an important example of how Congress can pursue an Appropriations Clause lawsuit, and how a court could favorably adjudicate these claims. The case thus underscores the *possibility* of these lawsuits being successful.

[112] *See* Burwell, 130 F. Supp. 3d at 69 ("[N]o case has decided whether this institutional plaintiff has standing on facts such as these."). Westlaw indicates that only 268 cases in federal courts have cited the Appropriations Clause. *See* Westlaw, http://next.westlaw.com (last visited Feb. 3, 2018) (click "Statutes & Court Rules," then "U.S. Constitution," then "Article I, Section 9, Clause 7," then "Citing References"; choose "Cases" and filter by "Federal"). Only one lawsuit brought by individual members of Congress has directly alleged a violation of the Appropriations Clause.*See* Harrington v. Schlesinger, 528 F.2d 455 (4th Cir. 1975). The past lawsuits against the ***Executive*** authorized by a body of Congress have all involved committees' subpoena and investigatory ***powers***. *See* ALISSA M. DOLAN & TODD GARVEY, CONG. RESEARCH SERV., R42454, CONGRESSIONAL PARTICIPATION IN ARTICLE III COURTS: STANDING TO SUE 11 (Sept. 4, 2014), http://www.fas.org/sgp/crs/misc/R42454.pdf [http://perma.cc/GK32-WYAS] ("[A]ll of the available cases regarding congressional institutions asserting an institutional injury have dealt with judicial enforcement of a subpoena.").

[113] and acknowledged that Congress has no legislative recourse where the President misappropriates funds. [114] Those developments suggest that a legislative Appropriations Clause suit is a live possibility for both Congress and the courts.

While *Burwell* is the most prominent successful Appropriations Clause claim against the ***Executive***, it is not the only one. In *United States v. McIntosh*, the Ninth Circuit recently held that criminal defendants could challenge the use of federal funds to prosecute them for marijuana crimes in violation of a congressional appropriations restriction. [115] If third parties like the defendants in *McIntosh* can use the Appropriations Clause to challenge fundamental ***executive powers***--prosecutorial discretion and enforcement of federal law--then Congress, the body imbued with ***power*** by the Appropriations Clause, should be able to use the clause to effectuate its role in our tripartite federal system. As will be **[*2535]** discussed in further detail later, a congressional suit would also show that Congress intended not to appropriate for the challenged activity, which could in turn make it easier for third parties to argue that point in their own cases. The partial success of these suits, and *Burwell* in particular, will signal to interested members of Congress that Appropriations Clause claims are judicially viable. Members of Congress that have sought relief through individual lawsuits in the past could then attempt to secure judicial resolution by framing a ***national security*** dispute as an Appropriations Clause violation. [116]

B. Appropriations Clause Challenges and Political Will

Beyond the emerging legal viability of these lawsuits, history demonstrates that they are also politically feasible. Of course, it is easy to imagine conditions under which Congress would be unlikely to muster the political will to pass appropriations restrictions or a resolution to sue the President for violating them. For example, if Congress is attempting to stop an existing military operation--such as in Libya in 2011--it may be particularly likely to fail. [117] Additionally, in times of unified government, the congressional majority would likely be hesitant to challenge the President of its own party.

At other times, though, the possibility of Appropriations Clause lawsuits is much more apparent. In times of divided government, Congress has strong political incentives to oppose the President with all of the tools at its disposal. [118] Over the last four decades, individual members of Congress have demonstrated their

---

[113] Burwell, 130 F. Supp. 3d at 71 ("[The] constitutional structure would collapse, and the role of the House would be meaningless, if the ***Executive*** could circumvent the appropriations process and spend funds however it pleases."); id. at 73.

[114] Id. at 73 (noting that the "the authority trespassed" here "is not statutory; it is constitutional" and Congress does not have "the authority to repeal or amend the terms of Article I, § 9, cl. 7").

[115] 833 F.3d 1163, 1174 (9th Cir. 2016).

[116] *See* Anthony Clark Arend & Catherine B. Lotrionte, *Congress Goes to Court: The Past, Present, and Future of Legislator Standing*, 25 HARV. J.L. & PUB. POL'Y 209, 281 (2001) ("[T]here will undoubtedly continue to be members of Congress who will take recourse to the courts.").

[117] *See* Steinhauer, *supra* note 38.

[118] *See, e.g.*, Douglas Kriner & Liam Schwartz, *Divided Government and Congressional Investigations*, 33 LEGIS. STUD. Q. 295, 297 (2008) (demonstrating that "interbranch tensions" and congressional investigations of the ***executive*** sharply increase in times of divided government).

willingness to seek judicial resolution of war ***powers*** and foreign affairs disputes; [119] and with the emerging viability of institutional Appropriations Clause **[*2536]** claims, they could seek congressional resolutions to pursue them. Indeed, on numerous occasions, houses of Congress have voted to institutionally oppose the ***executive*** branch in court. [120]

Congress has proven itself willing to oppose ***executive*** action by flexing its ***power*** of the purse in the ***national security*** context. In the 2016 Consolidated Appropriations Act, for instance, Congress passed a large number of appropriations restrictions dealing with a variety of ***national security*** issues. [121] Indeed, Congress routinely enacts identical appropriations restrictions in its annual appropriations bills. From at least 2012 onwards, for instance, every annual consolidated appropriations act has barred "funds made available by this Act" from being "used in contravention of the War ***Powers*** Resolution." [122] The annual consolidated appropriations acts contain numerous other ***national security***-related appropriations restrictions as well. [123]

[*2537] Furthermore, since 2014, these acts have more specifically limited presidential prerogatives to engage in specified military excursions in Syria. [124] Since 2015, the exact same restriction has been

---

[119] *See, e.g.*, Goldwater v. Carter, 444 U.S. 996 (1979) (challenging the President's unilateral termination of a treaty); Holtzman v. Schlesinger, 484 F.2d 1307 (2d Cir. 1973) (challenging the bombing in Cambodia during the Vietnam War); Kucinich v. Obama, 821 F. Supp. 2d 110 (D.D.C. 2011) (challenging military action in Libya).

[120] *See, e.g.*, Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076, 2103 (2015) (noting the U.S. Senate as amicus curiae); United States v. Windsor, 133 S. Ct. 2675 (2013); INS v. Chadha, 462 U.S. 919, 922 (1983) (noting the appearance of the U.S. Senate and the U.S. House of Representatives).

[121] For just some of the many restrictions enacted, see Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, §§ 8044, 8046, 8050, 8053, 8056, 8058, 8060, 8062, 8065, 8071, 8074, 8076, 8078-8081, 8106, 8122, 9007-9008, 9019, 129 Stat. 2242, 2362-2371, 2376, 2380, 2393, 2397 (2015).

[122] Consolidated Appropriations Act of 2017, Pub. L. No. 115-31, § 8104, 131 Stat. 135, 271 (2017); Act of 2016 § 8106, 129 Stat. at 2376; Consolidated and Further Continuing Appropriations Act of 2015, Pub. L. No. 113-235, § 8116, 128 Stat. 2130, 2280 (2014); Consolidated Appropriations Act of 2014, Pub. L. No. 113-76, § 8117, 128 Stat. 5, 132 (2014); Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. No. 113-6, § 8116, 127 Stat. 197, 326 (2013); Consolidated Appropriations Act of 2012, Pub. L. No. 112-74, § 8129, 125 Stat. 786, 838 (2011).

[123] Over the same period, every such act has prohibited any funds from being "expended for assistance to the Democratic People's Republic of Korea unless specifically appropriated for that purpose." Act of 2017 § 8045, 131 Stat. at 238; Act of 2016 § 8044, 129 Stat. at 2362; Act of 2015 § 8042, 128 Stat. at 2263; Act of 2014 § 8042, 128 Stat. at 115; Act of 2013 § 8042, 127 Stat. at 307; Act of 2012 § 8042, 125 Stat. at 816. Every act has prohibited funds for "international military education and training" and "peacekeeping operations" from being "used to support any military training or operations that include child soldiers." Act of 2017 § 8088, 131 Stat. at 267; Act of 2016 § 8088, 129 Stat. at 2372; Act of 2015 § 8092, 128 Stat. at 2275; Act of 2014 § 8116, 128 Stat. at 132; Act of 2013 § 8115, 127 Stat. at 326; Act of 2012 § 8128, 125 Stat. at 838. And every act has prohibited any funds from being expended to "establish any military installation or base for the purpose of providing for the permanent stationing of United States Armed Forces in Iraq" or Afghanistan, to "exercise United States control over any oil resource of Iraq," or to violate any U.S. laws that implement the Convention Against Torture. Act of 2017 §§ 9007-9008, 131 Stat. at 289; Act of 2016 §§ 9007-9008, 129 Stat. at 2393; Act of 2015 §§ 9007-9008, 128 Stat. at 2298; Act of 2014 §§ 9007-9008, 128 Stat. 147-48; Act of 2013 §§ 9007-9008, 127 Stat. at 339; Act of 2012 §§ 9007-9008, 125 Stat. at 850.

[124] Act of 2017 § 9019, 131 Stat. at 292; Act of 2016 § 9019, 129 Stat. at 2397; Act of 2015 § 9014, 128 Stat. at 2300 (providing that "[n]one of the funds made available by this Act may be used with respect to Syria in contravention of the War ***Powers*** Resolution (50 U.S.C. 1541 et seq.), including for the introduction of United States armed or military forces into hostilities in Syria, into situations in Syria where imminent involvement in hostilities is clearly indicated by the

enacted with respect to Iraq. [125] And there are numerous additional ***national security*** appropriations restrictions enacted each year, ranging from weapons [126] and intelligence issues [127] to military-base strength [128] and aid to foreign forces. [129]

Because Congress engages with appropriations every year, it has frequent opportunities to insert restrictions in anticipation of a conflict with the ***Executive***. Yearly appropriations also mean that Congress can be highly responsive to potential military excursions. Congress can thus enact a restriction when overseas tensions begin, before they fully escalate into a conflict. For example, the repeat provision prohibiting funds from being spent on hostilities in Syria [130] was re-enacted in the annual 2016 appropriations bill passed in December 2015, after tensions began in the region but more than a year before President Trump decided to engage in hostilities with the Syrian government. [131]

[*2538] Beyond Congress's demonstrated ability to enact appropriations restrictions, legislators have started to evince a commitment to changing how wars are funded and to reasserting Congress's role in authorizing military involvement abroad. There is growing discomfort on both sides of the aisle with wars being funded through the amorphous overseas contingency operations account, [132] and with the President's ability to carry out new unauthorized operations through the framework of the antiquated 2001 Authorization for the Use of Military Force (AUMF). [133] This is demonstrated by numerous co-sponsored

---

circumstances, or into Syrian territory, airspace, or waters while equipped for combat, in contravention of the congressional consultation and reporting requirements of" the WPR); Act of 2014 § 9015, 128 Stat. at 150.

[125] Act of 2017 § 8115, 131 Stat. at 274; Act of 2016 § 8122, 129 Stat. at 2380; Act of 2015 § 8140, 128 Stat. at 2285.

[126] Act of 2017 § 8019, 131 Stat. at 250 (demilitarizing "M-1 Carbines, M-1 Garand rifles, M-14 rifles, .22 caliber rifles, .30 caliber rifles, or M-1911 pistols"); *id.* § 8077, 131 Stat. at 265 (prohibiting funds for "research, development, test, evaluation, procurement or deployment of nuclear armed interceptors of a missile defense system").

[127] Act of 2015 § 8128, 128 Stat. at 2283 (prohibiting the use of funds by the NSA to target U.S. persons and acquire their electronic communications under FISA); Act of 2013 § 8123, 127 Stat. at 327 (prohibiting funds in contravention of acts "relating to sharing classified ballistic missile defense information with Russia").

[128] Act of 2015 § 8125, 128 Stat. at 2283 (specifying force structure at "Lajes Field, Azores, Portugal").

[129] Act of 2017 § 8131, 131 Stat. at 276 (prohibiting funds to be used "to provide arms, training, or other assistance to the Azov Battalion" in Ukraine).

[130] Act of 2016 § 9019, 129 Stat. at 2397.

[131] Dan Lamothe et al., *U.S. Strikes Syrian Military Airfield in First Direct Assault on Bashar al-Assad's Government*, WASH. POST (Apr. 7, 2017), http://www.washingtonpost.com/world/***national-security***/trump-weighing-military-options-following-chemical-weapons-attack-in-syria/2017/04/06/0c59603a-1ae8-11e7-9887-1a5314b56a08_story.html [http://perma.cc/8SU4-7Z6S]. The 2016 restriction is still in force under the continuing appropriations acts for FY2017.*See* Pub. L. No. 114-254, 114th Cong. (2016); Pub L. No. 114-223, 114th Cong. (2016).

[132] Stephanie Condon, *Pentagon "Slush Fund" Pays for ISIS Airstrikes, Irking Some in Congress*, CBS NEWS (Oct. 3, 2014, 6:00 AM), http://www.cbsnews.com/news/pentagon-slush-fund-pays-for-isis-airstrikes-irking-some-in-congress [http://perma.cc/QGE2-UZCE].

[133] Jake Miller, *John Boehner "Happy" To Have Congress Vote on Anti-ISIS Mission*, CBS NEWS (Sept. 28, 2014, 5:53 PM), http://www.cbsnews.com/news/john-boehner-happy-to-have-congress-vote-on-anti-isis-mission [http://perma.cc/V2F4-NT26].

efforts to reform the WPR, [134] prohibit expenditures for military action in the absence of congressional authorization, [135] prevent the expansion of troops into Syria, [136] repeal the 2001 AUMF, [137] and enact a new AUMF. [138] While most of these have not been **[*2539]** passed into law, they nonetheless signal that legislators of both parties are ready to change the way that wars are funded.

Even members of a President's political party may often disagree with the ***Executive***'s position on ***national security*** issues, particularly when the actions stop short of full-fledged armed conflict. [139] For example, in July 2017, the Republican-led Congress imposed sanctions on Russia against President Donald Trump's wishes. That bipartisan effort passed by a veto-proof majority in both houses. [140] And, as will be explored further below, [141] Congress prevented President Obama from closing or transferring prisoners out of Guantanamo throughout his presidency, even when Democrats controlled one or both chambers. When members of Congress develop a bipartisan consensus on a question of ***national security***, they have shown themselves willing to oppose a President who does not buy into that consensus.

Appropriations Clause lawsuits are thus feasible under many circumstances--particularly in times of divided government and outside the context of ongoing military operations--because Congress has demonstrated that it possesses the political will and appropriations tools to oppose the ***Executive***. Congress has been increasingly engaged in a robust bipartisan debate over its proper role in authorizing and funding ***national***

---

[134] War ***Powers*** Amendments of 2017, H.J. Res. 75, 115th Cong. (2017), http://www.congress.gov/115/bills/hjres75/BILLS-115hjres75ih.pdf [http://perma.cc/T798-9V7U].

[135] Reclamation of War ***Powers*** Act, H.R. 1448, 115th Cong. (2017), http://www.congress.gov/bill/115th-congress/house-bill/1448/text [http://perma.cc/4US7-EWNU] (prohibiting funds from being "expended for introduction of the Armed Forces into hostilities . . . in the absence of-- (A) a declaration of war; (B) specific statutory authorization; or (C) a national emergency").

[136] Prohibit Expansion of U.S. Combat Troops into Syria Act, H.R. 1473, 115th Cong. (2017), http://www.congress.gov/bill/115th-congress/house-bill/1473/cosponsors?q=%7B%22search%22%3A%5B%22fund+war+appropriations%22%5D%7D&r=62 [http://perma.cc/ZJ4L-CKDV] (indicating that the bill had thirty-three co-sponsors).

[137] Brian Bender & Jennifer Scholtes, *House Panel Votes To Force New Debate on Terror War*, POLITICO (June 29, 2017, 12:48 PM), http://www.politico.com/story/2017/06/29/congress-vote-authorize-war-islamic-state-240095 [http://perma.cc/7RDF-NBBR] (discussing the success of the amendment to repeal the 2001 AUMF before the House Appropriations committee by an overwhelmingly bipartisan vote); Sheryl Gay Stolberg,*Senate Rejects Bipartisan Effort To End 9/11 Military Force Declaration*, N.Y. TIMES (Sept. 13, 2017), http://www.nytimes.com/2017/09/13/us/politics/senate-rejects-rand-paul-effort-to-end-military-force-declaration.html [http://perma.cc/4G5E-X8XG] (discussing the failure of Senate and House efforts).

[138] Charlie Savage, *Senators Wrestle with Updating Law Authorizing War on Terrorist Groups*, N.Y. TIMES (June 20, 2017), http://www.nytimes.com/2017/06/20/us/politics/aumf-war-military-congress.html [http://perma.cc/5PFD-5G3N] (discussing, among other efforts, the Authorization for Use of Military Force Against al-Qaeda, the Taliban, and the Islamic State of Iraq and Syria, S.J. Res. 43, 115th Cong. (2017)).

[139] *See, e.g.*, David M. Herszenhorn, *Democrats in Senate Block Money To Close Guantánamo*, N.Y. TIMES (May, 19, 2009), http://www.nytimes.com/2009/05/20/us/politics/20detain.html [http://perma.cc/DJ2R-DKP3].

[140] Peter Baker & Sophia Kishkovsky, *Trump Signs Russian Sanctions into Law, with Caveats*, N.Y. TIMES (Aug. 2, 2017), http://www.nytimes.com/2017/08/02/world/europe/trump-russia-sanctions.html [http://perma.cc/RF62-Z5NY]; *see* Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, 131 Stat. 886 (2017).

[141] *See infra* notes 148-159 and accompanying text.

security measures, and has begun flexing its muscles vis-à-vis the President. Appropriations Clause litigation provides another vehicle for Congress to exercise its authority after appropriations are made. Moreover, the ex post threat of litigation would strengthen Congress's bargaining position and encourage the expanded enactment of appropriations restrictions in the first place.

C. Potential Applications

Assuming that congressional Appropriations Clause lawsuits are both legally feasible and politically possible, it still remains to be shown how they could be applied in practical terms. In terms of constitutional policy, these suits have the potential to vindicate separation-of-***powers*** principles and reassert Congress's **[*2540]** proper constitutional role in the ***national security*** context. [142] However, in order for Congress to bring such claims in the first instance, these suits must also have useful concrete applications.

There are various circumstances in which Congress could assert its authority through Appropriations Clause litigation to influence ***national security*** policy making. For example, appropriations litigation could effectuate congressional ***national security*** policy by enabling judicial enforcement of appropriations restrictions already in place, [143] such as the Leahy Amendments. [144] The Leahy Amendments prohibit the use of appropriations "for any training, equipment, or other assistance for the members of a unit of a foreign security force if the Secretary of Defense has credible information that the unit has committed a gross violation of human rights." [145] Lawsuits to enforce the Leahy laws directly would face substantial obstacles in the courts due to concerns about sovereign immunity, standing, and the political question doctrine. [146] However, congressional plaintiffs would avoid sovereign immunity concerns and have a greater chance of surpassing other procedural hurdles by arguing that any funds spent in violation of the Leahy Amendments were not appropriated, and therefore were spent in violation of the Constitution.

Another potential application of Appropriations Clause litigation would be to vindicate Congress's interpretation of the 2001 AUMF. Assume the President and Congress disagree over whether to interpret the AUMF as authorizing the use of force against ISIL. [147] In light of this dispute, Congress could enact an appropriations restriction prohibiting the use of funds to combat ISIL until an ISIL-specific authorization for the use of military force is enacted. Should the President disregard this restriction, Congress could bring an Appropriations Clause action to vindicate its position.

The transfer of five Guantanamo detainees in exchange for the release of Sgt. Bowe Bergdahl provides an even more concrete example. When President Obama was elected in 2008, he pledged to shut down the detention facility at **[*2541]** Guantanamo Bay, Cuba within his first year in office. His campaign promise,

---

[142] *See infra* Part VI.

[143] *See supra* notes 121-131 and accompanying text.

[144] Limitation on Assistance to Security Forces, 22 U.S.C. § 2378d (2006); Consolidated Appropriations Act of 2014, Pub. L. No. 113-76, § 8057, 128 Stat. 5, 118-19 (2014).

[145] Act of 2014 § 8057(a)(1).

[146] Nathanael Tenorio Miller, Note, *The Leahy Law: Congressional Failure,* ***Executive*** *Overreach, and the Consequences*, 45 CORNELL INT'L L.J. 667, 692 (2012).

[147] The assumption should not be all that difficult to conjure. *See, e.g.*, Letter from Senators Tammy Baldwin & Brian Schatz to President Barack Obama (Dec. 5, 2014) ("[W]e do not believe that you possess sufficient authority to undertake the current U.S. military campaign against ISIL.").

however, faced significant opposition in Congress, including from members of his own party. [148] Asserting a contrary policy position on this ***national security*** issue, Congress countered President Obama's proposed closure with its purse ***power***, passing a series of appropriations restrictions to block construction of an alternative detainee facility, and to prevent the transfer of detainees into the United States or to other countries without following notification and certification procedures. [149] Though President Obama contested the legality of these restrictions, [150] they nonetheless stymied his effort to close Guantanamo.

However, President Obama did not entirely abide by these restrictions. The Taliban held Bergdahl captive for five years in Afghanistan, until five Taliban detainees at Guantanamo were exchanged for his release. [151] That is to say, President Obama secretly transferred five Guantanamo detainees from the facility, without properly notifying Congress thirty days in advance, in violation of section 1035(d) of the National Defense Authorization Act of 2014, [152] and section **[*2542]** 8111 of the Department of Defense Appropriations Act of 2014. [153] And by spending $ 988,400 [154] to effectuate the transfer, contrary to an express appropriations restriction, the ***Executive*** also violated the Appropriations Clause. [155]

---

[148] Herszenhorn, *supra* note 139153.

[149] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, §§ 8103-8105, 129 Stat. 2242, 2376 (2015); Consolidated and Further Continuing Appropriations Act of 2015, Pub. L. No. 113-235, §§ 8112-8114, 128 Stat. 2130, 2280 (2014); Act of 2014, §§ 8110-8112, 128 Stat. at 131; Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. No. 113-6, §§ 8109-8111, 127 Stat. 197, 323 (2013); Consolidated Appropriations Act of 2012, Pub. L. No. 112-74, §§ 8119-8121, 125 Stat. 786, 833 (2011); Department of Defense and Full-Year Continuing Appropriations Act of 2011, Pub. L. No. 112-10, §§ 1112-1114, 125 Stat. 38, 114 (2011); Consolidated Appropriations Act of 2010, Pub. L. No. 111-117, § 532, 123 Stat. 3033, 3156 (2009).

[150] Statement on Signing the National Defense Authorization Act for Fiscal Year 2014, 2013 DAILY COMP. PRES. DOC. 876 (Dec. 26, 2013) (contending that transfer funding restrictions "violate[] constitutional separation of ***powers*** principles").

[151] Dan Lamothe, *The Bowe Bergdahl Case, Explained*, WASH. POST (Dec. 14, 2015), http://www.washingtonpost.com/news/checkpoint/wp/2015/12/14/how-to-catch-up-on-the-bowe-bergdahl-case [http://perma.cc/C2DD-L6Y5].

[152] National Defense Authorization Act of 2014, Pub. L. No. 113-66, § 1035(d), 127 Stat. 672, 853 (2013).

[153] Pub. L. No. 113-76, § 8111 (2014) ("None of the funds appropriated or otherwise made available in this Act may be used to transfer any individual detained at United States Naval Station Guantanamo Bay, Cuba to the custody or control of the individual's country of origin, any other foreign country, or any other foreign entity except in accordance with section 1035 of the National Defense Authorization Act for Fiscal Year 2014.").

[154] Memorandum from Susan A. Poling, Gen. Counsel, Gov't Accountability Office, to Sen. Mitch McConnell, at 3 (Aug. 21, 2014), http://www.gao.gov/assets/670/665390.pdf [http://perma.cc/NH95-ZN24].

[155] *See* David Bernstein, *Revisiting the Illegal Bowe Bergdahl Swap: Undermining Congress's "**Power** of the Purse,"* WASH. POST: VOLOKH CONSPIRACY (Dec. 10, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/10/revisiting-the-illegal-bergdahl-swap-undermining-congresss-***power***-of-the-purse [http://perma.cc/GAU7-34Q5]; Jack Goldsmith,*One or Two Other Statutes the President Likely Disregarded in The Bergdahl Deal*, LAWFARE (June 2, 2014), http://lawfareblog.com/one-or-two-other-statutes-president-likely-disregarded-bergdahl-deal-updated [http://perma.cc/3VAF-6DQT] (noting that the President's actions transferring Guantanamo detainees in exchange for Bergdahl, in addition to violating several statutes,**"**might also have violated Article I, § 9, cl. 7 of the Constitution").

Faced with this blatant statutory and constitutional violation, Congress had two potential responses: impeachment or political shaming. Though a few legislators floated the idea of impeachment, [156] such a severe sanction for saving the life of a U.S. serviceman was not politically feasible. Congress therefore chose less formal means of opposition. Legislators held hearings and made public statements. [157] The Government AccountabilityOffice issued a legal opinion concluding that the ***Executive*** had violated section 8111 and the Antideficiency Act, [158] and the House voted 249-163 (with 22 Democrats in favor) in a non-binding resolution to condemn the illegality of the transfer. [159] Those soft measures marked the end of Congress's objections: a fairly clear constitutional violation, **[*2543]** nullifying Congress's strongest ***power*** in the ***national security*** arena, turned into another instance of the ***Executive***'s accretion of ***power***.

However, Congress had a third choice: an Appropriations Clause suit against the President. The House, which had just passed a condemnatory resolution and which boasted a Republican majority that deeply opposed the President's Guantanamo policy, likely had the political will to pass a resolution to sue the President for violating the Appropriations Clause. The House could have sought a declaratory judgment of unconstitutionality and an injunction against any such future detainee transfers. And Congress's constitutional authority over ***national security*** funding would have possibly been vindicated, instead of eroded.

IV. THE MECHANICS OF APPROPRIATIONS CLAUSE LITIGATION IN THE *NATIONAL SECURITY* CONTEXT

Appropriations Clause litigation by congressional plaintiffs admittedly faces special hurdles in the ***national security*** context. In previous lawsuits involving Members of Congress challenging the President on matters of ***national security***, courts have employed standing doctrine, the political question doctrine, mootness, and ripeness to avoid reaching the merits. [160] Should a court reach the merits in such a dispute, it would be faced with the question of whether the President's expenditure was nonetheless constitutional because Congress's refusal to appropriate for a certain object violated the President's inherent discretionary ***power***. [161] This Part explores the requirements an Appropriations Clause lawsuit must satisfy and explores the affirmative steps Congress must take in order for these lawsuits to succeed, both at the jurisdictional stage and on the merits.

---

[156] *See* Jonathan Capehart, *Bergdahl and the GOP's Predictable Impeachable Offense*, WASH. POST (June 3, 2014), http://www.washingtonpost.com/blogs/post-partisan/wp/2014/06/03/bergdahl-and-the-gops-predictable-impeachable-offense [http://perma.cc/9TXY-RE3C].

[157] *See The Bergdahl Exchange: Implications for U.S.* ***National Security*** *and the Fight Against Terrorism: Hearing of the H. Foreign Affairs Comm. J. Subcomm.*, 113th Cong. (June 18, 2014), http://foreignaffairs.house.gov/hearing/joint-subcommittee-hearing-the-bergdahl-exchange-implications-for-u-s-***national-security***-and-the-fight-against-terrorism [http://perma.cc/ZQC4-37HX].

[158] *See* Memorandum from Susan A. Poling, *supra* note 154, at 1.

[159] Associated Press, *U.S. House Condemns Obama for "Illegal" Bowe Bergdahl Prisoner Swap*, GUARDIAN (Sept. 9, 2014), http://www.theguardian.com/world/2014/sep/09/us-house-obama-bowe-bergdahl-illegal-swap [http://perma.cc/W8NU-86DL].

[160] *See* FISHER, *supra* note 2, at 302; Harold Hongju Koh, *Judicial Constraints: The Courts and War* ***Powers****, in* THE U.S. CONSTITUTION AND THE ***POWER*** TO GO TOWAR, supra note 42, at 121, 122 ("[P]articularly after the Vietnam War . . . the federal courts have adopted an increasingly deferential attitude toward presidential warmaking.").

[161] *See* U.S. CONST. art. II, § 2, cl. 1 (Commander in Chief clause); *id*. art. II, § 1, cl. 1 (***Executive*** Vesting clause).

Even when examining the mechanics of Appropriations Clause lawsuits, broader issues of separation of ***powers*** remain. Many scholars claim that courts tend to give the political branches broad leeway in separation-of-***powers*** disputes, particularly on foreign affairs and on ***national security*** issues. [162] On this view, courts are often wary of wading into disputes between the branches in such **[*2544]** sensitive policy areas. They would therefore hesitate to entertain Appropriations Clause challenges involving ***national security*** if they believe it would overstep their role to do so.

However, courts have not shied away from confronting the ***Executive*** when ***national security*** interferes with constitutional rights or ***powers***, even during wartime. As Louis Fisher notes: "A close examination of judicial rulings over the last two centuries reveals that the automatic association of war ***power*** with the political question category is a misconception. Not only did courts decide war ***power*** issues, they sometimes spoke against the authority of the president." [163] Indeed, from a historical point of view, the frequent invocation of procedural roadblocks in the early Vietnam era was an aberration, rather than the rule. [164]

Furthermore, the judiciary appears to have regained its earlier willingness to hear ***national security*** cases. At the height of the War on Terror, the Supreme Court took four major cases from Guantanamo Bay detainees challenging their detentions and ruled against the Government each time. [165] In *Boumediene v. Bush*, the Court rejected claims that it should stay out of the political branches' way when dealing with issues of terrorism, even amidst an ongoing conflict. It stated that while "proper deference must be accorded to the political branches" in this area, "[t]he laws and Constitution are designed to survive, and remain in force, in extraordinary times." [166] More generally, the Court has been aggressive in defining the ***powers*** of its sister branches, whether over immigration, [167] the recognition of foreign countries, [168] the making of recess appointments, [169] the imposition of good-cause requirements on presidential appointments, [170] or the question of whether congressional involvement can maintain Article III adversity when the President refuses to defend a law against a private lawsuit. [171]

Lower courts have taken this message to heart in the recent battles over President Trump's ***executive*** order temporarily banning travel from specified countries. While according some deference to the

---

[162] *See, e.g.*, Edward Cantu, *The Separation-of-**Powers** and the Least Dangerous Branch*, 13 GEO. J.L. &PUB. POL'Y 1, 33-34 (2015); Harlan Grant Cohen, *A Politics-Reinforcing Political Question Doctrine*, 49 ARIZ. ST. L.J. 1, 12 (2017); Gillian E. Metzger, *The Constitutional Duty To Supervise*, 124 YALE L.J. 1836, 1908 (2015).

[163] Louis Fisher, *Judicial Review of the War **Power***, 35 PRESIDENTIAL STUD. Q. 466, 469 (2005).

[164] *Id.* at 484, 493.

[165] Boumediene v. Bush, 553 U.S. 723 (2008); Hamdan v. Rumsfeld, 548 U.S. 557 (2006); Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Rasul v. Bush, 542 U.S. 466 (2004).

[166] Boumediene, 553 U.S. at 796, 798.

[167] *E.g.*, Sessions v. Morales-Santana, 137 S. Ct. 1678 (2017).

[168] *E.g.*, Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076 (2015).

[169] *E.g.*, NLRB v. Noel Canning, 134 S. Ct. 2550 (2014).

[170] *E.g.*, Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477 (2010).

[171] *E.g.*, United States v. Windsor, 133 S. Ct. 2675 (2013).

Executive, courts adjudicating these **[*2545]** claims have asserted their role in determining constitutional questions. [172] Sensitivity about intruding into interbranch disputes, and into ***national security*** decision making, will always cause courts to think carefully before moving to the merits in these cases. But deciding whether an action is constitutional is "a familiar judicial exercise," and "courts cannot avoid their responsibility merely" because a case involves ***national security***. [173] And, whatever the courts' views on handling separation-of-***powers*** cases writ large, Appropriations Clause lawsuits provide a particularly clear and convenient way to resolve disputes between the political branches. [174] The clarity with which Congress could frame the problem in an appropriations bill and the fact that such a suit would involve basic statutory interpretation make those suits especially conducive to judicial review.

A. Jurisdictional and Threshold Issues

Before a court can reach the merits of an Appropriations Clause claim, it must have jurisdiction. Congressional plaintiffs may have to prove that they have standing, that the case is ripe, that the case is not moot, and that the political question doctrine does not apply. If one house or the entire Congress authorizes suit and follows certain procedures, an Appropriations Clause case should clear these hurdles.

1. Standing

The first specific hurdle to Appropriations Clause challenges is standing. One house of Congress could have standing to seek redress of an institutional injury, though a lawsuit brought by both houses would have the greatest chance of success, and a suit by individual members would almost surely fail.

A number of scholars and judicial opinions have debated the contours of legislative standing, [175] and have reached some consensus about the scope of the **[*2546]** doctrine. First, as *Raines v. Byrd* clearly establishes, [176] individual members of Congress do not have standing to pursue a separation-of-***powers*** claim. [177] In contrast, Congress should have standing to sue over institutional injuries if both houses voted to jointly bring the suit. [178] In separation-of-***powers*** cases, the President's failure to follow constitutional

---

[172] *See, e.g.*, Hawaii v. Trump, 859 F.3d 741, 768 (9th Cir.), *vacated as moot*, 138 S. Ct. 377 (Mem.) (2017); Int'l Refugee Assistance Project v. Trump, 857 F.3d 554, 590 (4th Cir.) (en banc), *vacated as moot*, 138 S. Ct. 353 (Mem.) (2017); Washington v. Trump, 847 F.3d 1151, 1161 (9th Cir.), *cert. denied sub nom*. Golden v. Washington, 138 S. Ct. 448 (Mem.) (2017).

[173] Zivotofsky ex rel. Zivotofsky v. Clinton, 566 U.S. 189, 196 (2012).

[174] *See supra* notes 93-101 and accompanying text.

[175] *See, e.g.*, Theodore Y. Blumoff, *Judicial Review, Foreign Affairs and Legislative Standing*, 25 GA. L.REV. 227, 307-22 (1991); Matthew I. Hall, *Making Sense of Legislative Standing*, 90 S.CAL. L. REV. 1 (2016); Bradford C. Mank, *Does a House of Congress Have Standing Over Appropriations? The House of Representatives Challenges the Affordable Care Act*, 19 U. PA. J.CONST. L. 141 (2016).

[176] 521 U.S. 811, 830 (1997).

[177] *See* Blumoff, *supra* note 175, at 311-12, 340-41; Hall, *supra* note 175, at 29-30; Mank, *supra* note 175, at 149. However, the doctrine of legislative standing may continue to develop to allow suits by groups of individual members of Congress, particularly where they represent a substantial voting bloc. For example, in June 2017 a group of 196 members of Congress filed a suit against President Trump alleging violations of the Emoluments Clause. Complaint, *Blumenthal v. Trump*, No. 17-cv-01154-EGS (D.D.C. June 14, 2017). Such lawsuits give the courts an opportunity to further develop this doctrine in a way that may make future appropriations litigation more feasible.

[178] *See* Blumoff, *supra* note 175, at 341; Hall, *supra* note 175, at 28; *see* Mank, *supra* note 175, at 166.

legislative processes inflicts a particularized injury on Congress as an institution. Recently, in *Arizona State Legislature v. Arizona Independent Redistricting Commission*, the Court determined that a state legislature challenging the creation of an independent redistricting commission in the state had standing as "an institutional plaintiff asserting an institutional injury": the legislature believed the Constitution gave it "'primary responsibility' for redistricting," and the initiative requiring the use of an independent commission "would 'completely nullif[y]' any vote by the Legislature . . . purporting to adopt a redistricting plan." [179] While the Court was careful not to decide the question in the case of Congress, [180] this recent opinion augurs well for congressional standing when a unified governmental institution brings suit. The Court has never outright held that Congress can sue the President, but the Court's cases have "clearly *implied* that Congress has standing to sue when the ***executive*** branch allegedly intrudes on core legislative authority." [181] This is particularly so when both houses of Congress have explicitly authorized suit, since that places the official imprimatur of the legislative branch on the action. [182]

A greater difficulty lies in determining whether a single house or committee would have standing to bring a separation-of-***powers*** suit in the appropriations context. The Court has not had to deal with such cases, so we must rely on the reasoning of the few cases it has decided, as well as the decisions of lower courts and the views of legal academics. Some scholars argue that Appropriations Clause cases can only be brought--if at all--by both houses of Congress, because **[*2547]** the appropriations ***power*** is vested in the entire Congress, not its constituent parts. [183] Others contend that one house can bring suit because the appropriations "process is a core institutional ***power*** of Congress and of the House of Representatives in particular, where appropriation bills are supposed to originate." [184]

The case law suggests that even a single chamber could bring a suit. First, there is *Raines v. Byrd* itself. *Raines* read a prior case, *Coleman v. Miller*, as holding that "legislators whose votes would have been sufficient to defeat (or enact) a specific legislative act have standing to sue if that legislative action goes into effect (or does not go into effect), on the ground that their votes have been completely nullified." [185] Each house of Congress must vote to authorize appropriations. Therefore, each house would have had to pass any appropriations bill that would have allowed the President to spend the misappropriated funds. By spending the money anyway, the President acts as though a piece of legislation--to which each house's assent is separately required--has gone into effect when it has not. [186] Each house therefore suffers an institutional injury when the President removes money from the Treasury without the approval of both chambers. This is the paradigmatic injury that legislative standing cases like *Raines* and *Coleman* have

---

[179] 135 S. Ct. 2652, 2663-65 (2015) (alteration in ***original***) (citation omitted).

[180] Id. at 2665 n.12.

[181] Mank, *supra* note 175, at 188-89 (emphasis added) (footnote omitted).

[182] Ariz. State Legislature, 135 S. Ct. at 2664; Blumoff, *supra* note 175, at 309.

[183] *See* Hall, *supra* note 175, at 42.

[184] *See* Mank, *supra* note 175, at 188.

[185] Raines v. Byrd, 521 U.S. 811, 823 (1997).

[186] United States v. Windsor, 133 S. Ct. 2675, 2713 (2013) (Alito, J., dissenting) ("Just as the state-senator-petitioners in *Coleman* were necessary parties to the [child labor constitutional] amendment's ratification, the House of Representatives [i]s a necessary party to [any appropriation's] passage; indeed, the House's vote would have been sufficient to prevent [the appropriation's] repeal if the [President] had not chosen to execute that repeal [by violating the appropriations statute].").

recognized as sufficient to bring suit: by violating the funding restrictions that their votes were necessary to put in place, the President would be "completely nullif[ying]" the legislators' votes. [187]

Lower court cases likewise suggest that a house of Congress or its authorized representative can establish standing to vindicate Congress's appropriations ***power***. In *United States v. AT&T*, the D.C. Circuit determined that a single house of Congress had standing to assert an institutional injury, and could authorize a single Member or Committee to sue on its behalf. [188] A number of other cases, including *Senate Select Committee on Presidential Campaign Activities v. Nixon*, [189] **[*2548]** *Committee on Oversight and Government Reform v. Holder*, [190] *Committee on Judiciary v. Miers*, [191] and *House of Representatives v. Department of Commerce*, [192] have allowed congressional committees to sue to vindicate Congress's institutional interest in enforcing its own subpoenas against the ***Executive***.

These cases provide ample support for a house of Congress--as opposed to the individual legislators in *Raines*--to obtain standing following a transgression of specific appropriations. [193] They also rebut the argument that Congress cannot bring Appropriations Clause cases because appropriations violations do not result in a permanent loss of legislative ***power***. [194] Just as Congress has standing to enforce individual subpoenas even though refusal to comply with a single subpoena does not eliminate Congress's subpoena ***power***, Congress has standing to sue over individual Appropriations Clause violations despite its continuing ***power*** to pass other appropriations.

A third set of cases, dealing with prudential standing, also hints at Congress's ability to maintain lawsuits against the ***Executive***. For instance, in *INS v. Chadha*, both houses of Congress voted in separate resolutions to intervene to defend the constitutionality of the legislative veto. [195] In response to the claim that the suit did not meet Article III's "case or controversy" requirement, because the INS agreed with Chadha that the legislative veto was unconstitutional, the Court said that the intervention of both houses of Congress placed "the concrete adverseness" required under Article III "beyond doubt." [196] Any prudential concerns about jurisdiction, the Court held, were likewise dispelled "by inviting and accepting briefs from both Houses of Congress." [197] Similarly, in *United States v. Windsor*, the House Bipartisan Legal Advisory

---

[187] Raines, 521 U.S. at 823.

[188] United States v. AT&T, 551 F.2d 384, 391 (D.C. Cir. 1976); *see also* U.S. House of Representatives v. Burwell, No. 14-1967, 2015 WL 5294762, at *10 (D.D.C. Sept. 9, 2015) (citing *AT&T*).

[189] 498 F.2d 725 (D.C. Cir. 1974).

[190] 979 F. Supp. 2d 1 (D.D.C. 2013).

[191] 558 F. Supp. 2d 53 (D.D.C. 2008).

[192] 11 F. Supp. 2d 76, 85 (D.D.C. 1998).

[193] Burwell, 130 F. Supp. 3d at 80 n.29 (D.D.C. 2015) ("While there is no precedent for this specific lawsuit, the rights of the House as an institution to litigate to protect its constitutional role has been recognized in other contexts in the 20th century and its institutional standing was most specifically foreseen, if not decided, in *Raines* and *Arizona Legislature*." (citations omitted)).

[194] Hall, *supra* note 175, at 41-42.

[195] INS v. Chadha, 462 U.S. 919, 930 n.5 (1980).

[196] Id. at 939.

[197] Id. at 940.

Group (BLAG) voted to intervene on behalf of the House once the ***Executive*** announced that it would no longer defend the Defense of Marriage Act (DOMA). [198] The Court asked the parties to brief the question of whether BLAG had standing to appeal the Second Circuit's **[*2549]** decision striking down DOMA. [199] It ultimately determined that the ***Executive*** had standing, and therefore did not reach the question in regard to BLAG. [200] However, to reach this conclusion the Court first held that "BLAG's sharp adversarial presentation of the issues satisfie[d] the prudential concerns that otherwise might counsel against hearing an appeal from a decision with which the principal parties agree." [201] While these cases did not directly deal with Article III standing, they strongly suggest that the Court recognizes that one or both houses may have sufficient interest in preserving Congress's legislative prerogative to justify continuing otherwise dubious lawsuits against the ***executive*** branch.

Furthermore, any opposition to congressional standing to bring separation-of-***powers*** lawsuits in the ***national security*** context is likely premised on the assumption that, even if courts are unavailable as a forum, Congress still has the "***power*** of the purse to protect its options." [202] This rationale is premised on Congress's being able to use the other tools at its disposal--especially appropriations--to resolve the interbranch conflict. But when the ***Executive*** violates the Appropriations Clause, nullifying the purse ***power***, litigation may provide the only means for Congress to vindicate its constitutional role. [203]

For a house of Congress to bring a future Appropriations Clause suit in a ***national security*** dispute, it would likely have to pass a resolution similar to that authorizing suit in *Burwell*. [204] Doing so would raise the prospect of an institutional injury and lay the groundwork for the legislators to claim standing to sue the President. Addressing the standing question, then, should ultimately be the same in the context of ***national security*** appropriations as in agency appropriations or investigatory ***powers*** and subpoena enforcement. [205] The cases addressed above demonstrate that a single house has a colorable standing argument on the basis of an appropriations violation. As the next Section argues, though, there **[*2550]** might be other benefits to both houses' suing together through a joint resolution.

2. Ripeness

---

198 United States v. Windsor, 133 S. Ct. 2675, 2684 (2013).

199 *Id.*

200 Id. at 2686-88.

201 Id. at 2688.

202 Blumoff, *supra* note 175, at 350.

203 Of course, another option is impeachment. But where appropriations misconduct has become standard ***executive*** practice in the ***national security*** space, impeachment may have become too blunt a tool to be politically and constitutionally feasible to redress this constitutional injury.

204 U.S. House of Representatives v. Burwell, 130 F. Supp. 3d 53, 63 (D.D.C. 2015); *see also* DOLAN & GARVEY, *supra* note 112, at 14.

205 *Cf.* Dornan v. U.S. Sec'y of Def., 851 F.2d 450, 451 (D.C. Cir. 1988) (noting that the courts have "not sharply defined how Congress as an institution claims its standing in an appropriate case," but implying that institutional standing for Congress is more likely than standing for individual members of Congress).

To reach the merits, a dispute must also have crystallized, or ripened, into one "fit[] . . . for judicial decision." [206] Although suit by one house alone may have sufficient standing, both houses of Congress may need to bring suit together to show that Congress fully opposes the President's expenditure of unappropriated funds and thereby establish ripeness. [207] In this case, the House and the Senate would only be able to bring an Appropriations Clause challenge together through passing a concurrent resolution.

While all of the jurisdiction and justiciability doctrines could create problems for ***national security*** plaintiffs, ripeness poses a particular hurdle to an Appropriation Clause suit. In *Goldwater v. Carter*, for example, a few members of Congress challenged the President's unilateral termination of a treaty. [208] Justice Powell would have dismissed the case as unripe, reasoning that "a dispute between Congress and the President is not ready for judicial review unless and until each branch has taken action asserting its constitutional authority" and the branches reach "a constitutional impasse." [209]

Following Justice Powell's "constitutional impasse" requirement, courts have dismissed claims brought by congressional plaintiffs against the ***Executive*** where Congress as a body has not already taken action against the President. [210] Relatedly, courts have been hesitant to find a case ripe when key factual questions remain unanswered. Most recently, in *Doe v. Bush*, the First Circuit ruled that a lawsuit by twelve members of the House, seeking to prevent the President from **[*2551]** starting a war against Iraq, was unripe because at the time "[m]any important questions remain[ed] unanswered about whether there w[ould] be a war, and, if so, under what conditions." [211] If the courts are convinced that political or factual predicates are underdeveloped, they might refuse to hear a case for ripeness reasons.

In an Appropriations Clause lawsuit, Congress can control the factual predicates to adjudication. If Congress passes an explicit restriction on appropriations, the President disregards the restriction, and congressional plaintiffs sue, the layers of speculation that doomed the *Doe* case will be cleared away. [212] Concurring in *Sanchez-Espinoza v. Reagan*, then-Judge Ginsburg specifically acknowledged the "***power***

---

[206] Nat'l Park Hosp. Ass'n v. Dep't of the Interior, 538 U.S. 803, 808 (2003).

[207] Sanchez-Espinoza v. Reagan, 770 F.2d 202, 211 (D.C. Cir. 1985) (Ginsburg, J., concurring) (affirming dismissal because "no gauntlet has been thrown down here by a majority of the Members of Congress"); Dellums v. Bush, 752 F. Supp. 1141, 1151 (D.D.C. 1990) ("[I]t is only if the majority of the Congress seeks relief from an infringement on its constitutional wardeclaration ***power*** that it may be entitled to receive it.").

[208] 444 U.S. 996, 997 (1979) (Powell, J., concurring).

[209] Id. at 996.

[210] *See* Dellums, 752 F. Supp. at 1149-52 (finding a challenge of fifty-four members of Congress to the President's imminent attack on Iraq to be unripe); Lowry v. Reagan, 676 F. Supp. 333, 339 (D.D.C. 1987) (noting the lack of ripeness under *Goldwater* within a discussion of remedial discretion); Crockett v. Reagan, 558 F. Supp. 893, 899 (D.D.C. 1982) (noting a lack of "constitutional impasse"), *aff'd*, 720 F.2d 1355 (D.C. Cir. 1983); *see also* Sanchez-Espinoza, 770 F.2d at 210 (Ginsburg, J., concurring) ("I would dismiss the 'war ***powers*** clause' claim for relief asserted by the congressional plaintiffs as not ripe for judicial review.").

[211] Doe v. Bush, 323 F.3d 133, 139 (1st Cir. 2003).

[212] However, if congressional plaintiffs alleged an Appropriations Clause violation on the basis that narrowly appropriated funds did not include this activity--rather than an explicit restriction--ripeness may present an issue. *See infra* text accompanying notes 259-262. In this situation, Congress might have to pass a joint resolution to the effect that the President is spending unappropriated funds in order for the dispute to be ripe. *See* Crockett, 558 F. Supp. at 899 (reasoning that if Congress passed a resolution regarding war ***powers*** that the President ignored, there would be a "constitutional impasse appropriate for judicial resolution").

of the purse" as a "formidable weapon[]" by which a majority of Congress could "throw[] down" the "gauntlet" to create a ripe dispute. [213] Therefore, an action pursuant to Congress's appropriations ***power*** would constitute an "asserti[on] . . . [of] constitutional authority," the violation of which constitutes a "constitutional impasse." [214] Congress need not take a further contrary action in the face of presidential overreach; the ***original*** funding restriction means that the branches have all acted.

The political predicates necessary for adjudication will also be satisfied if a majority of both houses of Congress brings suit. One court, in *Dellums v. Bush*, specifically contemplated that plaintiffs must "be or represent a majority of the Members of the Congress" in order to avoid a dismissal on ripeness grounds. [215] The presence of a majority of both houses as plaintiffs would indicate that Congress as a body views the President's actions as unconstitutional. Ultimately, if Congress takes the necessary steps to assert its appropriations ***power***, "ripeness should not pose a major barrier to judicial review" [216] in Appropriations Clause cases.

[*2552] *3. Mootness*

Even if a court makes it past questions of standing and ripeness, some suits--especially longer-running ones--may be moot. Mootness can prevent judicial adjudication of interbranch ***national security*** disputes because the challenged ***executive*** activity may cease before the courts can act. [217] For example, in *Conyers v. Reagan* eleven members of the House of Representatives challenged the invasion of Grenada in October 1983 as a violation of the War ***Powers*** Clause. [218] The district court dismissed on grounds of equitable discretion, and the congressional plaintiffs appealed. [219] However, by the time the D.C. Circuit decided the dispute, the conflict had ended: all combat troops had been withdrawn from Grenada, and only a small training contingent remained. [220] The D.C. Circuit held that claims for both declaratory and injunctive relief were moot. [221] Appropriations Clause lawsuits alleging that the President is spending unappropriated funds to engage in a military action may end up suffering the same mootness problem as *Conyers*.

Furthermore, Appropriations Clause cases may face another mootness issue: the annual expiration of appropriations. In *Sanchez-Espinoza v. Reagan*, twelve members of the House challenged ***executive*** aid to the Nicaraguan Contras, arguing in part that the President violated the Boland Amendment, a restriction

---

213 Sanchez-Espinoza, 770 F.2d at 211 (Ginsburg, J., concurring).

214 Goldwater, 444 U.S. at 996 (Powell, J., concurring).

215 Dellums, 752 F. Supp., at 1151.

216 Koh, *supra* note 160, at 124 (discussing the litigation of war ***powers*** disputes generally).

217 *See id*. at 125 (noting that because many Presidents have tried to keep unilateral military actions shorter than sixty days to avoid triggering the War ***Powers*** Resolution, many operations--like Libya (1986), Grenada, and Panama--are too short to be adjudicated).

218 765 F.2d 1124, 1125-26 (D.C. Cir. 1985).

219 Id. at 1126.

220 *Id.*

221 Id. at 1127-28; *see also* Lowry v. Reagan, 676 F. Supp. 333 (D.D.C. 1987), *aff'd*, No. 87-5426 (D.C. Cir. Oct. 17, 1988) (per curiam) (holding that the case presented a nonjusticiable political question and was moot on appeal).

on providing funds to the Contras that was included in the Fiscal Year 1983 appropriations bill. [222] However, because the appropriations bill expired at the end of 1983, and the plaintiffs sought only prospective relief, the D.C. Circuit dismissed the claim as moot. [223]

These applications of mootness might pose a problem for Appropriations Clause litigation that seeks to end a short military operation. However, extended conflicts or non-war ***powers*** disputes will not suffer this problem. Additionally, **[*2553]** there are two other ways that mootness might be avoided. First, plaintiffs could attempt to structure an argument for declaratory judgment in such a way as to avoid mootness. For example, in *Mitchell v. Laird* the D.C. Circuit suggested that "a declaratory judgment respecting past action" might avoid mootness, because "plaintiffs have a duty under the Constitution to consider whether defendants in continuing the hostilities did commit high crimes and misdemeanors so as to justify an impeachment." [224] Similarly, legislators might argue that they suffer a continuing injury when the ***Executive*** spends in violation of an appropriations restriction. The President's past action of withdrawing funds in violation of the Constitution institutionally injured Congress, and Congress has an ongoing duty to assess whether those actions are unconstitutional (and hence impeachment-worthy), with which courts can assist through a declaratory judgment. [225]

Second, even if courts do not view Appropriations Clause violations as continuing injuries, such cases could fall within the "capable of repetition, yet evading review" exception to mootness. [226] This doctrine allows suits to proceed when a case would otherwise be declared moot, if: (1) the challenged action is by nature too short-lived to allow for full litigation before the action ends, and (2) there is a reasonable expectation that the same plaintiff will be subject to the same action again. [227] The D.C. Circuit refused to use this exception in *Conyers*, because wars are not inherently so short that litigation cannot be completed before they end. [228] However, many ***national security*** matters begin and end within a much tighter timeframe than protracted conflicts. The transfer of prisoners from Guantanamo in exchange for Sergeant Bergdahl, for instance, occurred in secret and in a matter of days; no lawsuit could have occurred quickly enough to prevent the President from expending unappropriated funds before the expenditure occurred. And, given President Obama's known dislike of Guantanamo and the possibility that the ongoing wars in Iraq and Afghanistan could generate more prisoner swaps, it was reasonable to think that the President might transfer more detainees out of Guantanamo in the future. Therefore, if Congress had sued President Obama for unconstitutionally using funds in the Bergdahl exchange, it may well have avoided a mootness finding. When similar immediate and clandestine actions occur as part of a broader program, normal lawsuits can operate against the program as long as it still exists. But when they occur as a **[*2554]** series of one-off incidents, the capable of repetition but evading review doctrine could render them justiciable.

---

[222] 568 F. Supp. 596, 598 (D.D.C. 1983), *aff'd*, 770 F.2d 202 (D.C. Cir. 1985) (Scalia, J.). It appears that congressional plaintiffs structured this claim as a violation of the appropriations statute, not as a constitutional violation.

[223] Sanchez-Espinoza v. Reagan, 770 F.2d 202, 210. (D.C. Cir. 1985).

[224] 488 F.2d 611, 613 (D.C. Cir. 1973).

[225] *See also* Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477 (2010) (granting a declaratory judgment of unconstitutionality in lieu of injunctive relief to remedy a separation of ***powers*** injury).

[226] S. Pac. Terminal Co. v. Interstate Commerce Comm'n, 219 U.S. 498, 515 (1911).

[227] *See* Kingdomware Techs., Inc. v. United States, 136 S. Ct. 1969, 1976 (2016).

[228] Conyers v. Reagan, 765 F.2d 1124, 1129 (D.C. Cir. 1985); *see* Campbell v. Clinton, 203 F.3d 19, 33-34 (D.C. Cir. 2000) (Randolph, J., concurring).

Though Appropriations Clause lawsuits may not be able to prevent expenditures for a military operation that has already ended, congressional plaintiffs may still be able to vindicate their constitutional interests by bringing a claim for retrospective relief (such as reimbursement) that would not be moot. In order to avoid the mootness issue specific to annual appropriations, congressional plaintiffs would have to rely on narrowly structured appropriations, rather than on an overt restriction that would expire in a year; and the plaintiffs would have to argue that the appropriations did not provide funds for the action at issue. Alternatively, Congress could pass substantially similar restrictions every year, and plaintiffs could thereby plead an ongoing violation. Or Congress could simply attempt to pass a more permanent restriction.

Ultimately, the Supreme Court has cautioned that "[t]he burden of demonstrating mootness 'is a heavy one.'" [229] The ***Executive*** could have trouble meeting that burden in at least some Appropriations Clause cases if Congress legislates strategically.

4. Political Question Doctrine

The political question doctrine may pose a more significant problem for Appropriations Clause suits in the ***national security*** context than the core justiciability doctrines. Many interbranch ***national security*** disputes involving the War ***Powers*** Clauses have been found to present nonjusticiable political questions. [230] However, given the Supreme Court's renewed willingness to resolve constitutional claims on ***national security*** issues, a congressional Appropriations Clause suit could overcome the political question doctrine if the courts recognize the clear-cut statutory and constitutional questions such a case would present.

Courts have declined to resolve ***national security*** suits on various political-question rationales. In *Crockett v. Reagan*, for instance, twenty-nine members of Congress challenged military assistance in El Salvador as a violation of the WPR and the War ***Powers*** Clause. [231] The district court rejected the ***Executive***'s argument that the case presented a political question because it involved "potential judicial interference with ***executive*** discretion in the foreign affairs field" or "the **[*2555]** apportionment of ***power*** between the ***executive*** and legislative branches." [232] Nevertheless, the district court held that the case presented a nonjusticiable political question because the court "lacks the resources and expertise (which are accessible to the Congress) to resolve disputed questions of fact concerning the military situation in El Salvador." [233] The D.C. Circuit affirmed the decision. [234]

Courts considering War ***Powers*** challenges have also dismissed on the basis of the political question doctrine when they determine that they should not "substitute [their] judgment for that of the President, who

---

[229] County of Los Angeles v. Davis, 440 U.S. 625, 631 (1979) (quoting United States v. W. T. Grant Co., 345 U. S. 629, 633 (1953)).

[230] *See supra* note 57.

[231] Crockett v. Reagan, 558 F. Supp. 893, 895 (D.D.C. 1982).

[232] Id. at 898.

[233] *Id.*

[234] Crockett v. Reagan, 720 F.2d 1355, 1357 (D.C. Cir. 1983) (per curiam); *see also* Sanchez-Espinoza v. Reagan, 770 F.2d 202, 210 (D.C. Cir. 1985) (holding that dismissal of the War ***Powers*** claim at issue was required by *Crockett*); Holtzman v. Schlesinger, 484 F.2d 1307, 1310 (2d Cir. 1973) (finding a nonjusticiable political question in part because the case involved "questions of fact involving military and diplomatic expertise not vested in the judiciary").

has an unusually wide measure of discretion in" foreign affairs. [235] And they have found nonjusticiable political questions where adjudication would risk "the potentiality of embarrassment … from multifarious pronouncements by various departments on one question." [236]

However, as noted above, [237] these instances of judicial reticence form a minority of ***national security*** cases. Most of the time, courts have been willing to decide separation-of-***powers*** disputes on security matters. In *Baker v. Carr*, for instance, the Court surveyed its foreign affairs and duration-of-hostilities cases to develop the contours of the modern political question doctrine. [238] The Court concluded that, when "clearly definable criteria for decision may be available"--even in ***national security*** cases--"the political question barrier falls away." [239] This has proven true over time: the Court has repeatedly been willing to decide the merits of cases that subject the security decisions of the political branches to constitutional scrutiny. [240]

[*2556] Furthermore, the recent revival of judicial involvement in this area has led courts to address even core war-making issues. For instance, a more recent War ***Powers*** case in which the political question issue was addressed took a different tone than prior cases. In *Dellums v. Bush*, the district court determined that the case did not present a political question, reasoning that courts are not prohibited from determining whether the country is at "war" simply because the determination involves foreign affairs. [241] The district court noted that "courts have historically made determinations about whether this country was at war." [242] Therefore, even the central determination of whether the country is engaged in ongoing hostilities is susceptible to judicial resolution.

Whatever the status of other ***national security*** questions, an Appropriations Clause lawsuit could fare better than a War ***Powers*** lawsuit. Instead of being directed at the existence or imminence of a "war," a famously difficult question to resolve, an Appropriations Clause challenge would involve a "pure question[] of constitutional interpretation, amenable to resolution by" the courts, [243] for which there are clearly "manageable standards" for adjudication. [244] Indeed, courts have some experience adjudicating

---

[235] Mitchell v. Laird, 488 F.2d 611, 616 (D.C. Cir. 1973); *see* Holtzman, 484 F.2d at 1310.

[236] Lowry v. Reagan, 676 F. Supp. 333, 340 (D.D.C. 1987) (quoting Baker v. Carr, 369 U.S. 186, 217 (1962)), *aff'd*, No. 87-5426 (D.C. Cir. 1988) (per curiam).

[237] *See infra* note 240 and accompanying text.

[238] Baker, 369 U.S. at 211-14.

[239] Id. at 214.

[240] *See, e.g.*, Boumediene v. Bush, 553 U.S. 723 (2008) (detention of terrorist suspects); United States v. District Court, 407 U.S. 297 (1972) (***executive*** intelligence gathering); N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (prohibitions on publication of security secrets); Kent v. Dulles, 357 U.S. 117 (1958) (passport denial based on security determinations); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) (domestic reach of war ***powers***).

[241] 752 F. Supp. 1141, 1146 (D.D.C. 1990).

[242] *Id.*; *see also* KOH, *supra* note 5, at 220 (observing that federal courts since the Founding have "reviewed the legality of military seizures, presidential orders in wartime, retaliatory strikes, covert actions, ***executive*** agreements, and treaty interpretation").

[243] U.S. House of Representatives v. Burwell, 130 F. Supp. 3d 53, 79 (D.D.C. 2015).

[244] *Id.* (internal quotation marks omitted) (quoting Powell v. McCormack, 395 U.S. 486, 548-49 (1969)).

Appropriations Clause disputes. [245] These cases involve statutory interpretation and "constitutional review of ***Executive*** actions," applying standards with which courts are very "familiar." [246]

The political question doctrine, therefore, is not the imposing barrier it might seem to be. The Supreme Court has become more muscular in brushing aside political question claims in ***national security*** cases over the past two decades, returning to its pre-Vietnam Era norm. Most recently, in *Zivotofsky v. Kerry*, the Court reiterated that "[n]o policy underlying the political question doctrine suggests that Congress or the ***Executive*** … can decide the constitutionality of a **[*2557]** statute." [247] The same holds true for the constitutionality of ***executive*** actions that conflict with the appropriations ***power***. The courts' "duty will sometimes involve the '[r]esolution of litigation challenging the constitutional authority of one of the three branches,' but courts cannot avoid their responsibility merely 'because the issues have political implications.'" [248] Judges "have repeatedly recognized" through the years that "the constitutionally mandated function of the judiciary is at least as important, and, in [some judges'] view even more important, in times of national emergency than in ordinary times." [249] Though issues of constitutional conflict and ***executive*** deference may arise at the merits stage in these cases, [250] they should not prevent Appropriations Clause cases from reaching the merits.

B. Merits

On the merits, an Appropriations Clause suit presents one main factual question and one main legal question. Factually, the court will have to determine whether the President spent funds that were not appropriated. Legally, the court will have to determine whether the President violated the Constitution, or had the inherent authority to spend funds under Article II.

1. How To Establish that Funds Were Not Appropriated

It would be easiest for congressional plaintiffs to succeed on the first, factual question if Congress had previously passed a restriction on appropriations, prohibiting spending for a particular object. [251] Such a

---

[245] *See, e.g.*, Nevada v. Dep't of Energy, 400 F.3d 9, 13, 15 (D.C. Cir. 2005) (determining whether a particular statute constituted a "continuing appropriation," and whether funds from a general account may be appropriated for a specific purpose).

[246] Burwell, 130 F. Supp. 3d at 80 ("[T]he mere fact that the House of Representatives is the plaintiff does not turn this suit into a non-justiciable 'political' dispute."); *cf*. Meyer, *supra* note 53, at 118 ("[T]he courts are surely no less able to read and interpret the constitutional text in many congressional cases than when they interpret other broad or ambiguous constitutional provisions.").

[247] 566 U.S. 189, 196-97 (2012) (second alteration in ***original***) (quoting INS v. Chadha, 462 U.S. 919, 941-42 (1983)).

[248] *Id.* at 196 (alteration in ***original***) (quoting Chadha, 462 U.S. at 943).

[249] Stephen Reinhardt, *The Judicial Role in* ***National Security***, 86 B.U. L. REV. 1309, 1313 (2006).

[250] *See infra* Section V.B.

[251] *See, e.g.*, Foreign Assistance Act of 1973, Pub. L. No. 93-189, S 30, 87 Stat. 714, 732 ("No funds authorized or appropriated under this or any other law may be expended to finance military or paramilitary operations by the United States in or over Vietnam, Laos, or Cambodia."); *see also* BANKS & RAVEN-HANSEN, *supra* note 15, at 172 ("From colonial America we inherited not only a tradition of specific ***national security*** appropriations, but also the restrictive appropriation rider--a substantive legislative amendment or provision tacked onto a military appropriation, forcing the

restriction would constitute a "complete denial provid[ing] that no appropriated funds may be used for an activity that otherwise would be a proper object of expenditure from a lump-sum **[*2558]** appropriation for the agency." [252] Under this scenario, the court would engage in straightforward statutory interpretation to determine whether the restriction constituted a decision not to appropriate the funds that the President ultimately spent. Congress would have the greatest success if the restriction employed were broad and simple. [253]

Though an explicit restriction on funding would make it easiest for congressional plaintiffs to succeed in appropriations litigation, this method could also present some difficulties. First, Congress must have already passed the restriction--if it has not done so by the time the President begins spending, there may be a significant gap in time before congressional plaintiffs could bring an Appropriations Clause lawsuit. Second, appropriations restrictions are subject to presidential veto, meaning that any restriction with which the President disagrees would need support from a two-thirds majority in each house. [254] As discussed above, however, Congress successfully passes multiple appropriations restrictions in every appropriations bill, in advance of their actually being violated. [255] If Congress continues this practice and tries to anticipate potential ***national security*** issues in advance, express appropriations restrictions would be a viable basis for an Appropriations Clause suit. And unlike a standalone restriction passed in direct anticipation of litigation, a restriction included in must-pass annual funding bills would be far more likely to avoid the President's veto pen.

Alternatively, Congress could argue that existing appropriations do not cover the President's activities. [256] However, in the modern history of appropriations, Congress "has by statute or by acquiescence left broad presidential discretion to finance activities for which it has not made specific appropriation." [257] Thus, in **[*2559]** order to succeed on this argument, Congress would first have to reform the structure of its ***national security*** appropriations. As Banks and Raven-Hansen contend, "Congress has lacked the will, or--given the obscure nature of the customary and statutory authority for the discretion--the knowledge to eliminate" Presidents' latitude in ***national security*** spending. [258]

---

executive to take the bitter with the sweet."); *id.* at 54 (noting that such appropriation restrictions "have become almost routine" after the Vietnam War).

[252] Stith, *supra* note 23, at 1361.

[253] *Id.* at 1361 n.86 (noting the argument that the second Boland amendment "did not by its terms encompass the ***National Security*** Council in the White House" and opining that "[w]here the intent is to deny all funds for a particular object, it would be desirable not to include unnecessary descriptive language (which may be construed as terms of limitation)"); *see also* KOH, *supra* note 5, at 129 ("When, as in the case of the Boland amendments, the language of the restriction becomes more or less inclusive over time, ***executive*** officials can claim that the provision's vagueness impairs their ability to determine whether particular activities are proscribed.").

[254] *See* KOH, *supra* note 5, at 131.

[255] *See supra* notes 130-131 and accompanying text (Syria); *supra* notes 149-155 and accompanying text (Bergdahl).

[256] *See* Stith, *supra* note 23, at 1363 n.95 ("Is failure to appropriate any money the same as an explicit denial of appropriations? The answer is 'no' if the unmentioned activity is nonetheless within the terms of activities that are funded.").

[257] BANKS & RAVEN-HANSEN, *supra* note 15, at 170; *see supra* Section I.A.

[258] *Id.* at 175.

For congressional plaintiffs to successfully argue that a presidential action exceeded the statutory mandate, Congress would have to curtail presidential discretion and move from lump-sum appropriations back to a system of more specific appropriations. One means of accomplishing this could be to incorporate "line itemization and specific descriptions of spending objectives"--informal controls that are used in the determination of ***national security*** appropriations [259]--into appropriations statutes themselves. Congress has successfully done this before: in the 1991 and 1992 DOD Appropriations Acts, Congress provided that "classified spending restrictions" that laid out the budget specifications for secret or black budget programs in a committee report "shall have the force and effect of Law." [260] In addition to incorporating committee itemization and descriptions into appropriations statutes--in effect creating "smaller buckets"--Congress would have to scale back or explicitly restrict emergency or contingency funds. In light of bipartisan opposition to the use of these contingency funds, and growing bipartisan efforts to assert Congress's role in ***national security***, [261] this reform is becoming increasingly possible.

Should Congress successfully undertake these reforms, congressional plaintiffs may be able to establish that existing appropriations did not appropriate funds for expansive ***executive*** excursions. This would mean that Congress would not have to amass the political will to pass a new express funding restriction in anticipation of litigation. Consequently, the President would have one less opportunity to stymie the suit through her veto ***power***. A reformation of the structure of ***national security*** appropriations, reversing decades of modern practice, would likely be more difficult to accomplish than one explicit funding restriction, which Congress is already in the habit of enacting. However, political will seems to be amassing in favor of a new ***national security*** appropriations **[*2560]** scheme. And once in place, it would enable congressional plaintiffs to seek adjudication of appropriations violations as soon as the President exceeds her statutory prerogative.

Under this narrow appropriations framework, congressional plaintiffs would argue that--although not specifically denied funding--the President's activity was "with[out] the terms of activities that [we]re funded." [262] Though a more difficult exercise of statutory interpretation than that accompanying an "explicit restriction," it is by no means beyond the competency of the courts. [263]

2. Constitutional Dispute

In addition to the factual question--whether unappropriated funds were spent--the court must resolve the legal dispute--whether the President violated the Constitution in spending unappropriated funds, or whether the restriction itself was unconstitutional. Congress does not have unbounded authority to oversee the ***Executive*** through appropriations. [264] For example, "Congress is obliged to provide public funds for

---

[259] *Id.* at 63.

[260] Pub. L. No. 101-511, S 8111(a), 104 Stat. 1856 (1990); BANKS &RAVEN-HANSEN, *supra* note 15, at 65; *see also* Stith, *supra* note 23, at 1353 ("Often, the appropriations act explicitly incorporates other legislation. . . .").

[261] *See supra* notes 132131-138 and accompanying text.

[262] Stith, *supra* note 23, at 1363 n.95 (emphasis omitted).

[263] *See, e.g.*, Nevada v. Dep't of Energy, 400 F.3d 9, 15 (D.C. Cir. 2005) (adjudicating whether funds appropriated in a general account could be spent for a specific purpose).

[264] BANKS & RAVEN-HANSEN, *supra* note 15, at 144 ("Congress may not use ***national security*** appropriations to accomplish what it may not constitutionally do directly.").

constitutionally mandated activities." [265] Additionally, Congress cannot use appropriations restrictions to unduly interfere with the President's constitutional ***powers***. For ***national security*** purposes, the ***power*** of Congress is limited "in the degree to which it can interfere with the commander in chief's ***power*** to control military strategy." [266]

The Supreme Court has never conclusively resolved the question of whether an appropriations restriction unconstitutionally interferes with the President's ***national security powers***. [267] At least one lower court, however, has held that the President's constitutional authority over ***national security*** constrains Congress's ability to restrict funding. In *National Federation of Federal Employees v. United **[*2561]** States*, Congress prohibited the use of funds to enforce federal employee nondisclosure agreements that prevented Congress from receiving classified ***national security*** information. [268] The district court struck down this appropriations restriction, ruling that it unconstitutionally infringed on the President's authority over ***national security*** information as "head of the ***Executive*** Branch and as Commander in Chief." [269] However, "[i]n spite of the importance of the constitutional question whether [the restriction] impermissibly intrudes upon the ***Executive***'s authority to regulate the disclosure of ***national security*** information," the Supreme Court remanded without expressing an opinion because the controversy became moot. [270] *Federal Employees* has left "unclear how far Congress may go in exercising or enforcing its appropriations ***power*** to constrain the [P]resident's authorities in foreign affairs." [271] But it suggests that Congress may face some limits in reining in the President.

In adjudicating a ***national security*** appropriations dispute on the merits, congressional plaintiffs will face similar arguments in favor of presidential discretion. For example, the ***Executive*** may argue that "the President has an implied ***power*** to incur claims against the Treasury to the extent minimally necessary to perform his duties and exercise his prerogatives under article II." [272] This claim of an inherent spending ***power***, through widely criticized, [273] might make a congressional suit more difficult. The ***Executive*** may argue, as former Attorney General William Barr has, that "Congress 'ultimately only has the ***power*** to

---

[265] Stith, *supra* note 23, at 1350-51 ("For instance, in the area of foreign affairs, Congress itself would violate the Constitution if it refused to appropriate funds for the President to receive foreign ambassadors or to make treaties.").

[266] Ackerman & Hathaway, *supra* note 3, at 457; *see* BANKS & RAVEN-HANSEN, *supra* note 15, at 150 ("[T]here is a broad scholarly consensus that Congress may not interfere with the president's day-to-day command of an authorized war or defense against sudden attack.").

[267] David A. Simon, *Ending Perpetual War? Constitutional War Termination **Powers** and the Conflict Against al Qaeda*, 41 PEPP. L. REV. 685, 746 (2014).

[268] Nat'l Fed'n of Fed. Emps. v. United States, 688 F. Supp. 671, 685 (D.D.C. 1988), *vacated sub nom*. Am. Foreign Serv. Ass'n v. Garfinkel, 490 U.S. 153 (1989); *see* Pub. L. No. 100-202, S 630, 101 Stat. 1329, 1329-432 (1987).

[269] Nat'l Fed'n of Fed. Emps., 688 F. Supp. at 685 (quoting Dep't of Navy v. Egan, 484 U.S. 518, 527 (1988)).

[270] Garfinkel, 490 U.S. at 158.

[271] KOH, *supra* note 5, at 129.

[272] Sidak, *supra* note 102, at 1194.

[273] See BANKS &RAVEN-HANSEN, *supra* note 15, at 166-68; Stith, *supra* note 23, at 1352.

provide a lump sum' for the constitutional activities of the president," [274] and that any further restrictions are an inherent violation of presidential discretion. Particularly if congressional plaintiffs are relying on a narrow-appropriations theory, rather than an explicit restriction, the ***Executive*** could also urge the courts to **[*2562]** apply language from *United States v. Curtiss-Wright*, [275] "as a canon of deferential statutory interpretation," [276] to conclude that the presidential activity was within the ambit of the funding outlay. [277]

The courts would ultimately have to balance the ***Executive***'s arguments about its constitutional ***powers*** over ***national security*** [278] against the congressional plaintiffs' arguments about the constitutional ***powers*** of Congress over ***national security*** and appropriations. [279] "To determine the constitutionality of a restrictive ***national security*** appropriation," courts would likely "weigh the extent to which the restriction prevents the president from accomplishing constitutionally assigned functions against the need for the same restriction to promote objectives within the authority of Congress." [280]

The outcome of this constitutional analysis will depend on the object of the appropriations restriction. [281] For example, appropriations restrictions directed at ***national security*** issues apart from war making are unlikely to "prevent[] the president from accomplishing constitutionally assigned functions." Consider Leahy vetting: the Leahy Amendments prohibit the use of appropriations to train foreign security forces who have committed human rights violations. It is highly unlikely that a President could allege that this vetting process prevents her from "accomplishing constitutionally assigned functions," so as to outweigh Congress's appropriations ***power*** and policy objectives. Therefore, courts should find **[*2563]** that such appropriations restrictions are within the constitutional authority of Congress.

---

[274] BANKS & RAVEN-HANSEN, *supra* note 15, at 144 (quoting Panel Discussion, *The Appropriations* ***Power*** *and the Necessary and Proper Clause*, 68 WASH. U. L.Q. 623, 631 (1990) (remarks of William Barr)).

[275] United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) ("[C]ongressional legislation . . . must often accord to the President a degree of discretion and freedom from statutory restriction [in foreign affairs] which would not be admissible were domestic affairs alone involved.").

[276] KOH, *supra* note 5, at 138.

[277] *But see* Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076, 2090 (2015) (cutting back on the *Curtiss-Wright* doctrine of ***executive*** deference in foreign affairs, reasoning that "[t]he ***Executive*** is not free from the ordinary controls and checks of Congress merely because foreign affairs are at issue").

[278] *See* U.S. CONST. art. II, S 2, cl. 1(Commander-in-Chief clause); *id.* art. II, S 1, cl. 1 (***Executive*** Vesting clause); Fleming v. Page, 50 U.S. (9 How.) 603, 615 (1851) ("[The President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy.").

[279] *See supra* Section I.A.

[280] BANKS & RAVEN-HANSEN, *supra* note 15, at 146 (relying on the standard set forth in Justice Kennedy's concurrence in Pub. Citizenv. U.S. Dep't of Justice, 491 U.S. 440, 484 (1989) (Kennedy, J., concurring)).

[281] *See id.* at 148-57 (concluding that, under the separation of ***powers*** analysis, the 1984 Boland amendment and the 1973 funding cutoff to the Vietnam War are constitutional, whereas the 1970 restriction on the introduction of ground troops into Laos and Thailand would be unconstitutional).

Cutting off funding for a war presents a closer question. Consider for example Congress's attempt to prevent funds from being spent on a military conflict in Syria. [282] It directly juxtaposes Congress's ***power*** to declare war and to appropriate for the army and navy against the ***executive***'s Commander-in-Chief ***power***. Nonetheless, Congress would have a strong argument that declining to appropriate for military action in Syria does not "prevent[] the president from accomplishing constitutionally assigned functions." Declining to appropriate funds for a military conflict in its entirety does not unduly interfere with the President's prerogative as Commander-in-Chief. Congress is merely keeping chained the "Dog of war," [283] not attempting to control troop movements on the battlefield. [284] An appropriation restriction does not actually bar the President from pursuing a military effort; rather, she must go through the process of consulting with Congress and obtaining authorization and specific appropriations for this particular conflict. And requiring the President to follow this dialogic process is consistent with the distribution of constitutional war ***powers*** and burdens designed by the Framers. An attempt to exert more granular control--such as by prohibiting a raid on a specific stronghold--would cross the line into impermissibly commandeering the Commander-in-Chief ***power***. But by declining to appropriate at a broad level, Congress is merely exercising its constitutional prerogative to determine when funds can be released from the treasury. Therefore, where Congress is restricting appropriations that do not involve war ***powers***, or that involve high-level, general funding for a conflict, it could succeed in establishing that the restriction is within its constitutional authority and does not unduly impinge upon the President's constitutional authority.

[*2564] *3. Relief*

Should congressional plaintiffs win on the merits, either declaratory or injunctive relief may be available. [285] A declaratory judgment in this context would state that that Congress had not appropriated certain funds, but that by engaging in certain conduct the President was drawing unappropriated funds from the Treasury in violation of Article I, Section 9, Clause 7. This remedy would essentially formalize the signaling function of these lawsuits: it communicates that the President is violating the Constitution, and provides a focal point for the political response of Congress and the public. Although there is no enforcement mechanism by which courts can carry out their mandate against the ***Executive***, Presidents nearly always obey court orders due to their "moral force" and the "significant political cost" of disobeying. [286] And just as the shame of norm violation induces agencies to comply with court orders to avoid contempt findings, [287] the political shame and pressure of rule-of-law norms give declaratory judgments of unconstitutional ***executive*** action their potent effect. The threat of this ex post pronouncement of guilt would strengthen

---

[282] *See supra* note 124.

[283] Jefferson, *supra* note 17, at 397.

[284] Because battlefield commands clearly fall within the ambit of the Commander-in-Chief Clause, whereas the ability to authorize military action in a particular theater can arguably fall at least in part within Congress's ***power*** under the Declare War Clause, it is likely that the former but not the latter would be seen as a situation "where the Constitution by explicit text commits the ***power*** at issue to the exclusive control of the President," and thus where the courts "have refused to tolerate *any* intrusion by the Legislative Branch." Pub. Citizen, 491 U.S. at 485 (Kennedy, J., concurring in the judgment).

[285] Koh, *supra* note 160, at 124.

[286] Jonathan R. Siegel, *Suing the President: Nonstatutory Review Revisited*, 97 COLUM. L. REV. 1612, 1690 (1997).

[287] Nicholas R. Parrillo, *The Endgame of Administrative Law: Governmental Disobedience and the Judicial Contempt* ***Power***, 131 HARV. L. REV. 685, 777 (2018).

Congress's position ex ante, and make Presidents less willing to risk an Appropriations Clause suit by violating funding restrictions.

The second type of relief a court could order is a negative injunction. In *Dellums v. Bush*, Judge Greene declared that, "in principle, an injunction may issue at the request of Members of Congress to prevent the conduct of a war which is about to be carried on without congressional authorization." [288] Professor Harold Koh has opined that *Dellums* "clearly la[id] the groundwork for future requests for injunctive relief." [289] An injunction would apply equally to an Appropriations Clause lawsuit, in which the practical effect of blocking expenditures may be to cut off a war or to end a particular government program. For example, the *Burwell* court issued a decision on the merits of the House's Appropriations Clause claim in May 2016, holding that the Affordable Care Act did not permanently appropriate the reimbursement funds at issue. [290] To enforce its decision, the court "enjoin[ed] the use of unappropriated monies to fund reimbursements **[*2565]** owed to insurers under Section 1402" of the Act. [291] That *Burwell* enjoined the administration from acting based on Congress's refusal to make annual appropriations only strengthens the case for the availability of injunctive relief in cases in which Congress continues to reauthorize the same annual appropriations restrictions. [292] Presidential transgressions of Congress's repeated funding preferences would bolster the case for judicial resolution via an injunction. Habitual presidential overreach would be proof that the interbranch conflict was unresolvable in the political sphere--precisely the cases where judicial resolution is appropriate.

There is some doubt as to whether an injunction could be entered directly against the President for Appropriations Clause violations. The Supreme Court stated in 1866 that the courts lack jurisdiction over requests to "enjoin the President in the performance of his official duties," although they may entertain suits to enjoin the performance of a "purely ministerial act." [293] Subsequent cases have reaffirmed this conclusion. [294] There might be an argument that the simple act of withdrawing funds from the Treasury--separate from ***executive*** decision making that the funds should be spent on a specific policy objective--should be considered a "ministerial" act. [295] Regardless, an injunction could certainly be entered against the Secretary of the Treasury or the Secretary of Defense. [296] Furthermore, if an injunction were entered against a President or cabinet members but the President persisted in violating the court order, although

---

[288] Dellums v. Bush, 752 F. Supp. 1141, 1149 (D.D.C. 1990).

[289] Koh, *supra* note 160, at 122.

[290] U.S. House of Representatives v. Burwell, 185 F. Supp. 3d 165, 168 (D.D.C. 2016).

[291] *Id.*

[292] Id. at 174-75.

[293] Mississippi v. Johnson, 71 U.S. (4 Wall.) 475, 498, 501 (1866).

[294] *See* Franklin v. Massachusetts, 505 U.S. 788, 802 (1992); Hawaii v. Trump, 859 F.3d 741, 788 (9th Cir.), *vacated as moot*, 138 S. Ct. 377 (Mem.) (2017); Int'l Refugee Assistance Project v. Trump, 857 F.3d 554, 605 (4th Cir.) (en banc), *vacated as moot*, 138 S. Ct. 353 (Mem.) (2017).

[295] *See* Mississippi, 71 U.S. at 498-99.

[296] *See* Franklin, 505 U.S. at 802 (citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) to show that the Court held President Truman's action unconstitutional and enjoined the Secretary of Commerce); Hawaii, 859 F.3d at 788 (upholding the constitutionality of an injunction against the Secretary of Homeland Security and the Secretary of State); Int'l Refugee Assistance Project, 857 F.3d at 605-06 (holding that the District Court abused its discretion by including President Trump in its preliminary injunction).

the court likely could not "imprison the President for contempt," it could order other officials "to behave as though the President had obeyed the ***original*** injunction" and then punish them for contempt. [297]

[*2566] A third potential form of relief, beyond negative injunctions or declaratory judgments, is reimbursement via affirmative injunction. The argument for such relief stems from the nature of the injury: the President has allegedly spent money from the Treasury that Congress did not appropriate. As Congress is the keeper of the purse, the President must return what was taken without its permission. In the event that an affirmative injunction claim for reimbursement succeeds, the President would have to find funds to "return" to that Treasury account--perhaps from ***national security*** contingency funds--and those funds would be impounded for the rest of the fiscal year. The possibility of this remedy is supported by a proposal from Professor Nicholas Parrillo, who posits that contempt fines against agencies can likely be paid out from agency appropriations rather than from the general governmental Judgment Fund. [298] Similarly, a contempt fine against the Secretary of Defense for violating a court order barring him from using unappropriated funds could be paid out from general defense appropriations. And if judgments in the form of contempt fines can be paid from appropriations, it is possible that judgment in the form of an affirmative injunction could require reimbursement of misspent funds, in the form of ordering impoundment of equivalent funds from a contingency account. If the ***Executive*** then runs out of funds due to this reimbursement, it would have to return to Congress to request further appropriations--as the Constitution required in the first instance.

Importantly, as the preceding discussion shows, a house of Congress would not have to settle for a political remedy for an Appropriations Clause violation. That is critical given that a suit would only arise when the political branches are at an impasse. Normally, under the equitable-remedial discretion doctrine, "[w]here a congressional plaintiff could obtain substantial relief from his fellow legislators through the enactment, repeal, or amendment of a statute, the court should exercise its equitable discretion to dismiss the legislator's action." [299] Courts have previously used this doctrine to dismiss ***national security*** lawsuits brought by congressional plaintiffs. [300] Those courts reasoned that a lawsuit was **[*2567]** inappropriate where congressional plaintiffs could instead resort to "appropriations legislation, independent legislation or even impeachment." [301] However, in *Dellums v. Bush*, a district court reasoned that, where cutting off funding or impeachment is "politically or practically" unavailable, these legislative remedies could not serve as the basis for an exercise of remedial discretion. [302]

---

[297] Siegel, *supra* note 286, at 1690. *But see* Parrillo, supra note 287, at 739-57 (noting that courts have the ***power*** to imprison agency officials for contempt in principle but seldom exercise it).

[298] *See* Parrillo, *supra* note 287, at 735-39.

[299] Dornan v. U.S. Sec'y of Def., 851 F.2d 450, 451 (D.C. Cir. 1988) (per curiam) (citation omitted).

[300] *See id.*; Crockett v. Reagan, 720 F.2d 1355, 1357 (D.C. Cir. 1983) (per curiam) (affirming dismissal of claim based on equitable discretion because "congressional plaintiff's dispute is primarily with his or her fellow legislators"); Lowry v. Reagan, 676 F. Supp. 333, 337-39 (D.D.C. 1987), *aff'd on othergrounds*, No. 87-5426 (D.C. Cir. Oct. 17, 1988); Conyers v. Reagan, 578 F. Supp. 324 (D.D.C. 1984), *aff'd on other grounds*, 765 F.2d 1124 (D.C. Cir. 1985); United Presbyterian Church v. Reagan, 557 F. Supp. 61, 64 (D.D.C. 1982), *aff'd on othergrounds*, 738 F.2d 1375 (D.C. Cir. 1984) (challenging legality of E.O. 12333). *But see* Dellums v. Bush, 752 F. Supp. 1141, 1149 (D.D.C. 1990) ("A joint resolution counselling the President to refrain from attacking Iraq without a congressional declaration of war would not be likely to stop the President from initiating such military action if he is persuaded that the Constitution affirmatively gives him the ***power*** to act otherwise.").

[301] Conyers, 578 F. Supp. at 327.

[302] Dellums, 752 F. Supp. at 1149.

There are several reasons why judicial--as opposed to political--resolution is appropriate for ***national security*** appropriations violations. [303] First, the availability of appropriations legislation is itself considered a reason to exercise equitable discretion; however, if this check on ***executive*** behavior has failed, that is evidence that political resolution is not forthcoming. [304] Impeachment, on the other hand, is too extreme to be a realistic step that must be exhausted before bringing suit. [305] Second, the concept of equitable discretion does not cleanly apply when there are institutional plaintiffs, because such cases do not involve an individual who could seek relief from "his fellow legislators." [306] If the entire Congress is aggrieved, there is not an intrabranch remedy available. Third, *Burwell* indicates that the courts are less likely to (and should not) apply equitable-remedial discretion in the Appropriations Clause context. In its motion to dismiss, the Government invoked equitable discretion, arguing that the District **[*2568]** Court should make the House pursue "legislative means available to counter the ***Executive*** Branch." [307] The court rejected this argument in a footnote, reasoning that "the constitutional violation of which the House complains has the collateral effect of disarming the most potent of those legislative means." [308] Appropriations Clause violations, in other words, are different: Congress has *already* exhausted its most potent political tool short of impeachment, and can therefore seek judicial relief where it might not be able to otherwise.

*C. Appropriations Clause Suits and the Separation of **Powers***

As we have now seen, congressional Appropriations Clause suits have a good chance of making it past the procedural hurdles that have stymied prior lawsuits attempting to correct presidential overreach in the ***national security*** sphere. And, if preceded by strategic legislating, such suits have an even better chance of succeeding on the merits. This outcome would be entirely consistent with--and, indeed, could help streamline--the Supreme Court's framework for assessing separation-of-***powers*** challenges. As discussed earlier, if Congress were to clearly and narrowly appropriate funds for ***national security*** purposes, or to expressly prohibit an expenditure, then a presidential action in violation of those restrictions would fall into *Youngstown*'s category three, where ***executive power*** is at its "lowest ebb." [309] As Justice Jackson recognized in *Youngstown*, appropriation of funds--even regarding ***national security***--is a ***power*** the

---

[303] Meyer, *supra* note 53, at 91 n.139 ("[W]ere the President to refuse to obey legislation denying funds or troops to a particular war effort, the courts may again be faced with the question of whether individual members of Congress could sue or whether they should muster the necessary members to pass further legislation or to impeach.").

[304] *See* THE FEDERALIST NO. 58, supra note 15, at 357.

[305] *See* Tom Campbell, ***Executive*** *Action and Nonaction*, 95 N.C. L. REV. 553, 577, 601 (2017) (arguing that judicial resolution is often more inappropriate than the exercise of a "political weapon" like impeachment because as a weapon it is "too strong" and not every inter-branch dispute is "political in nature"); Michael Sant'Ambrogio, *Legislative Exhaustion*, 58 WM. & MARY L. REV. 1253, 1305 (2017) ("[G]iven the high political costs, Congress should reserve impeachment for truly egregious conduct. Impeachment should not be the congressional response to a sincere presidential belief . . . ."); Bethany R. Pickett, Note, *Will the Real Lawmakers Please Stand Up: Congressional Standing in Instances of Presidential Nonenforcement*, 110 NW. U. L. REV. 439, 467 (2016) ("[T]he President may be a popular president whose performance is exemplary in every other area. Judicial intervention is preferable to impeachment because it addresses the President's particular area of wrongdoing, instead of broadly attacking the President . . . ." (footnote omitted)).

[306] Dornan v. U.S. Sec'y of Def., 851 F.2d 450, 451 (D.C. Cir. 1988) (per curiam).

[307] Defendants' Memorandum in Support of Their Motion to Dismiss the Complaint at 26, U.S. House of Representatives v. Burwell, 130 F. Supp. 3d 53 (D.D.C. 2015) (No. 14-cv-01967-RMC).

[308] Burwell, 130 F. Supp. 3d at 79 n.28.

[309] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

Constitution commits wholly to Congress: "Congress alone controls the raising of revenues and their appropriation and may determine in what manner and by what means they shall be spent for military and naval procurement." [310] A congressional appropriations restriction on specific ***national security*** spending is the paradigmatic exercise of congressional authority that Justice Jackson recognized in *Youngstown*. If Congress could establish that it exercised this ***power***, presidential action to the contrary would violate the separation of ***powers***, as squarely dictated by Justice Jackson's canonical *Youngstown* concurrence.

It is true that Appropriations Clause lawsuits combine separation of ***powers*** and ***national security***, two areas of traditional judicial abdication. But, ironically, **[*2569]** Appropriations Clause lawsuits are likelier to succeed than many other separation-of-***powers*** or ***national security*** cases. Unlike many other provisions of the Constitution, the Court has recognized that the Clause involves a "straightforward and explicit command." [311] This gives the judiciary an easily administrable test for the familiar judicial exercise of constitutional interpretation. [312]

Just as importantly, the Court has noted that the Appropriations Clause was designed "as a restriction upon the disbursing authority of the ***Executive*** department"; [313] its very purpose is "to assure that public funds will be spent according to the letter of the difficult judgments reached by *Congress* as to the common good." [314] In so doing, the Clause prevents the ***Executive*** from replacing Congress's judgment with its own. The D.C. Circuit has also recognized that the Clause is "particularly important as a restraint on ***Executive*** Branch officers," and has called it "a bulwark of the Constitution's separation of ***powers*** among the three branches." [315] It would be ironic for the courts to invoke the separation of ***powers*** as a reason to avoid adjudicating straightforward disputes under a constitutional provision so precisely designed to empower one branch and rein in another.

This last point hints at the broader theoretical issues that Appropriations Clause litigation implicates. The courts have developed each of the procedural roadblocks discussed above in the ***national security*** context because they held a particular view of the separation of ***powers*** and of the judiciary's role. The view the courts developed was an understandable one. As seen throughout this Part, many of the cases that triggered restrictive procedural rules involved individual draftees or members of Congress trying to get courts to declare the existence or the conduct of a military action unconstitutional--requests almost uniquely designed to provoke judicial recoil. To prevent abuse of the judicial forum, the courts adopted a more restrictive attitude toward their own role vis-à-vis the other branches. This attitude was unusual as a historical matter [316] and reached beyond what was necessary to rein in frivolous cases.

---

[310] Id. at 643-44 ("While Congress cannot deprive the President of the command of the army and navy, only Congress can provide him an army or navy to command.").

[311] Office of Pers. Mgmt. v. Richmond, 496 U.S. 414, 424 (1990) (quoting Cincinnati Soap Co. v. United States, 301 U.S. 308, 321 (1937)).

[312] *See* Zivotofsky ex rel. Zivotofsky v. Clinton, 566 U.S. 189, 201 (2012).

[313] Cincinnati Soap, 301 U.S. at 321.

[314] Richmond, 496 U.S. at 428 (emphasis added).

[315] U.S. Dep't of Navy v. Fed. Labor Relations Auth., 665 F.3d 1339, 1347 (D.C. Cir. 2012).

[316] *See supra* text accompanying notes 163-164.

[*2570] More recently, however, the courts have returned to a more robust vision of the judicial role in both separation-of-***powers*** [317] and ***national security*** [318] disputes. Bringing suits under the Appropriations Clause could both reinforce and shape this trend. In discussing the ***Executive***'s decision to decline to defend statutes, for instance, the Court in *Windsor* sounded a larger theme about the importance of adjudication in interbranch conflicts. "[W]hen Congress has passed a statute and a President has signed it," the Court said, "it poses grave challenges to the separation of ***powers*** for the ***Executive*** at a particular moment to be able to nullify Congress'[s] enactment solely on its own initiative and without any determination from the Court." [319] The President's failure to follow congressional appropriations is exactly the sort of unilateral nullification about which the *Windsor* Court cautioned. Judicial engagement with Appropriations Clause lawsuits is thus a natural outgrowth of the Court's developing view of the separation of ***powers***. But because they involve relatively narrow disputes over whether certain expenditures were authorized, such suits can actually help courts minimize the interbranch friction that might otherwise grow without intervention.

To see why this is so, consider Justice Scalia's dissent in *Windsor*. The dissent advocated for a restrictive view of congressional standing, based on the Vietnamera conception of the courts' role. Rather than look to the courts, Justice Scalia said, Congress should confront the President politically--through "the elimination of funding," among other methods. [320] The problem with this logic, however, is that it provides no answer to the inevitable follow-up question: what happens if the President ignores Congress's funding command? To the extent the restrictive view of judicial ***power*** provides an answer to this question, that answer is to tell Congress to take even more extreme measures: to deny all funding to the ***Executive***, refuse to confirm presidential appointments, [321] or even impeach the President.

To be fair, Justice Scalia seemed to realize the herculean nature of this task. [322] But a majority on the current Court, as well as in the lower courts, appears to **[*2571]** recognize that the judiciary need not totally abandon the field--even in ***national security*** cases. [323] After all, Congress cannot use its appropriations ***power*** to confront the President, as Justice Scalia suggested, if the President thinks she can simply transfer funds to evade Congress's prescriptions. The *Burwell* court recognized this catch-22: "The political tug of war anticipated by the Constitution depends upon Article I, § 9, cl. 7 having some force." [324] By abstaining, as the restrictive view of the judiciary would require, the courts would either consign Congress to passing toothless appropriations restrictions or encourage the political branches to needlessly escalate their battles. Appropriations Clause lawsuits between Congress and the President would funnel

---

[317] *See, e.g.*, Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076 (2015); NLRB v. Noel Canning, 134 S. Ct. 2550 (2014); United States v. Windsor, 133 S. Ct. 2675 (2013); Zivotofsky ex rel. Zivotofsky v. Clinton, 566 U.S. 189 (2012); Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477 (2010).

[318] Kerry, 135 S. Ct. 2076; Clinton, 566 U.S. 189; cases cited *supra* note 165.

[319] Windsor, 133 S. Ct. at 2688.

[320] Id. at 2705 (Scalia, J., dissenting).

[321] *Id.* ("Nothing says 'enforce the Act' quite like ' . . . or you will have money for little else.'").

[322] *Id.* ("And by the way, if the President loses the lawsuit but does not faithfully implement the Court's decree, just as he did not faithfully implement Congress's statute, what then? Only Congress can bring him to heel by . . . what do you think? Yes: a direct confrontation with the President.").

[323] *See supra* notes 163-171 and accompanying text.

[324] U.S. House of Representatives v. Burwell, 130 F. Supp. 3d 53, 73 (D.D.C. 2015).

otherwise intractable debates over ***national security powers*** into narrower, justiciable disputes over funding, while giving legal teeth to the ***power*** of the purse.

V. BENEFITS INDEPENDENT OF SUCCESS

Even if an Appropriations Clause suit does not reach and succeed on the merits, the very initiation of ***national security*** appropriations litigation could positively influence behavior in three ways: (1) by encouraging narrower appropriations; (2) by acting as a signaling device; and (3) by rebutting any claim that Congress has consented to the ***Executive***'s attempts to distort or ignore their appropriations restrictions. Thus, while a successful suit would have the most impact, the benefits of a suit could accrue even if courts reject the suit for one of the reasons that have knocked out legislative suits in the past.

A. Encouraging Narrow Appropriations

As discussed above, the first step in Congress's bringing an Appropriations Clause suit would be for legislators to pass a narrow appropriations bill or an appropriations restriction. The potential to bring lawsuits on a theory of narrow appropriations could incentivize Congress to appropriate narrowly in the first instance, in case the need for adjudication should arise. [325] Those narrower ***national security*** appropriations would independently promote good governance. By limiting presidential spending discretion, and ensuring that the President **[*2572]** does not have unbridled control over appropriated funds to start an unauthorized military conflict, the ***Executive*** is faced with a clearer choice: seek appropriations from Congress, or unconstitutionally spend unappropriated funds. Structuring the President's decision in this fashion would offer a powerful incentive for the ***Executive*** to spend within constitutional bounds. One might question why this is relevant if the remedy to any potential violation is absent--that is, if an Appropriations Clause suit could be dismissed on justiciability grounds. However, there are various informal tools that Congress could leverage that an Appropriations Clause suit would bring into sharper relief. The full panoply of methods of congressional control are only available, though, if legislators circumscribe the wide berth that the current appropriations process grants the President; even the possibility that legislators could use narrowed appropriations in a suit would incentivize this critical first step.

It might seem that narrowing its appropriations could in itself solve Congress's problem, and obviate the need for Appropriations Clause lawsuits. However, the very threat of litigation--either by Congress itself or by third parties directly subject to the ***Executive***'s actions--is still an important backstop, in case the ***Executive*** does not respect the narrowed appropriations. There are two situations in which this may occur. The President or a cabinet secretary may refuse to abide by Congress's will and interpret the relevant statute to have made the appropriation in question. [326] This divergence of interpretations occurred recently in *House of Representatives v. Burwell*: the Secretary of Health and Human Services inferred, from "extra-textual" evidence, that appropriations were available to reimburse insurers under the Affordable Care Act. The district court found that Congress did not appropriate those funds and that the appropriation was thus unconstitutional. [327] Similarly, after Congress passed the Rohrabacher-Farr Amendment--which prohibited the use of federal funds to prevent states from implementing medical marijuana laws--the Obama Administration read the rider to prohibit only actions against states themselves, rather than against medical

---

[325] Or at the very least, to codify by reference committee reports with specified anticipated expenditures, to selectively enforce them if violated. *See* BANKS & RAVEN-HANSEN, *supra* note 15, at 65.

[326] This statutory interpretation may either be a good faith dispute between branches over the meaning of the text, or a less-than-good-faith interpretation motivated by the policy preferences of the branches.

[327] U.S. House of Representatives v. Burwell, 185 F. Supp. 3d 165, 168 (D.D.C. 2016).

marijuana providers or buyers. [328] Congress demanded an investigation **[*2573]** of this "tortuous twisting of the text," but was unsuccessful in changing the Administration's mind until the courts agreed with Congress in multiple challenges brought by criminal defendants. [329]

Alternatively, the President could try to ignore a narrow appropriation by claiming that it violates one of her exclusive and enumerated ***powers***. This occasionally occurs with respect to appropriations unrelated to ***national security***. For instance, once the courts rejected the Obama Administration's narrow reading of the Rohrabacher-Farr Amendment, Congress reauthorized the rider, and President Donald Trump issued a signing statement saying he would "treat this provision consistently with [his] constitutional responsibility to take care that the laws be faithfully executed." [330] Attorney General Jeff Sessions then sent a letter to Congress, arguing that the rider interfered with the President's authority to enforce the Controlled Substances Act. [331] Such constitutional claims are particularly likely to be made in the areas of foreign affairs and ***national security*** because of the historical assignment of ***executive*** primacy in those areas. For instance, President George W. Bush objected to an appropriations rider prohibiting the use of funds to cooperate with the International Criminal Court: in a signing statement, President Bush said he would only apply the rider when it was "consistent with [his] constitutional authority in the area of foreign affairs." [332] As discussed in Section III.C, President Obama violated the terms of another appropriations rider by using government funds to remove prisoners from Guantanamo, and argued that his inherent ***executive powers*** gave him freedom to arrange prisoner transfers. [333]

Particularly in ***national security*** situations, then, Presidents are often tempted to push their ***powers*** to the constitutional boundary. In the appropriations context, this manifests in the argument that Presidents have the inherent authority to transfer or spend funds in furtherance of their foreign affairs and **[*2574]** defense policies--even when Congress has expressly forbidden the use of funds for the Presidents' activities. Unitary executivists contend that the President must be allowed to fully exercise these ***powers***, despite Congress's appropriations authority. [334] The threat of a lawsuit, even one that might well fail, generates political and legal risk that may be necessary to force the ***Executive*** into compliance with lawful congressional appropriations. And the possibility of using such lawsuits as a tool would give Congress an extra incentive to appropriate more narrowly at the outset.

---

[328] *See* Christopher Ingraham, *Federal Court Tells the DEA To Stop Harassing Medical Marijuana Providers*, WASH. POST: WONK BLOG (Oct. 20, 2015), http://www.washingtonpost.com/news/wonk/wp/2015/10/20/federal-court-tells-the-dea-to-stop-harassing-medical-marijuana-providers [http://perma.cc/74VM-H99J].

[329] *Id.*; *see* United States v. McIntosh, 833 F.3d 1163, 1176-77 (9th Cir. 2016).

[330] *Statement by President Donald J. Trump on Signing H.R. 244 into Law*, OFF. PRESS SECRETARY, WHITE HOUSE (May 5, 2017), http://www.whitehouse.gov/the-press-office/2017/05/05/statement-president-donald-j-trump-signing-hr-244-law [http://perma.cc/L58Z-SLFP].

[331] *See* Christopher Ingraham, *Jeff Sessions Personally Asked Congress To Let Him Prosecute Medical-Marijuana Providers*, WASH. POST (June 13, 2017), http://www.washingtonpost.com/news/wonk/wp/2017/06/13/jeff-sessions-personally-asked-congress-to-let-him-prosecute-medical-marijuana-providers [http://perma.cc/J48E-WFKP].

[332] George W. Bush, *Statement on Signing the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002*, GOV'T PUBLISHING OFF. (Nov. 28, 2001), http://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2-doc-pg1458.pdf [http://perma.cc/7FQJ-H8TR].

[333] *See* Statement on Signing the National Defense Authorization Act for Fiscal Year 2014, *supra* note 150.

[334] *See, e.g.*, Sidak, *supra* note 102, at 1194.

B. Acting as a Signaling Device

Second, the possibility of a lawsuit can serve as a valuable signal from Congress. Congress can use its ***powers***--including both its appropriations and oversight authority--to signal its priorities to the ***Executive*** and the judiciary. [335] Approving lawsuits to enforce their appropriations riders, even if those lawsuits are not successful, would serve as a powerful warning to the President, agencies, the public, and even other members of Congress that appropriations restrictions must be taken seriously, and that a coordinate branch of government believes that the President is exceeding his constitutional authority.

The threat of an Appropriations Clause lawsuit in itself may be an effective tool by which Congress can influence presidential action. As it stands, the President may face political consequences or potential impeachment for violating the Appropriations Clause, but these can be difficult swords for Congress to wield without public awareness and support. The formal potential for judicial enforcement of the Appropriations Clause adds a weapon to the congressional arsenal. Even if actual legal consequences were unlikely, the President would have a stronger incentive to comply with congressional ***national security*** actions when Congress signaled that it wanted to limit ***executive*** spending ***power*** and that it would seek judicial redress to enforce those limits. For example, "President Bush sought congressional approval only weeks after the court ruled in *Dellums v. Bush*" that a challenge to the Iraq War was not ripe, instead of risking that the lawsuit could ripen and congressional plaintiffs could be granted an injunction. [336] The signal to the President is made all the stronger if Congress both appropriates narrowly *and* takes formal legal means to enforce appropriations. **[*2575]** While those signals are noisier when Congress is successful in court, they are nonetheless present even before a court hears the suit.

Similarly, although the War ***Powers*** Resolution (WPR) has proven legally unenforceable in practice, [337] and Presidents have uniformly contested its constitutionality, [338] it has nevertheless influenced political norms. Presidents often provide disclosures to Congress consistent with the WPR, [339] and ***executive*** branch officers are frequently called upon to offer explanations of how ***executive*** actions were consistent with the WPR--requests with which they routinely comply. [340] The WPR has not proven itself the strong legal tool envisioned, but it is nonetheless a potent political tool; it assists Congress in forcing the ***Executive*** to offer reasoned explanations for its unilateral war making, and brings separation-of-***powers*** principles to the political fore in every such disagreement. The threat of even unsuccessful Appropriations Clause

---

[335] *See, e.g.*, Charles M. Cameron & B. Peter Rosendorff, *A Signaling Theory of Congressional Oversight*, 5 GAMES &ECON. BEHAV. 44 (1993); Eugenia Froedge Toma, *Congressional Influence and the Supreme Court: The Budget as a Signaling Device*, 20 J. LEGAL STUDS. 131, 131-32 (1991).

[336] Meyer, *supra* note 53, at 75 n.47.

[337] *See* Crockett v. Reagan, 558 F. Supp. 893, 898-901 (D.D.C. 1982); *see also supra* note 52 and accompanying text.

[338] *See* HOWELL & PEVE HOUSE, *supra* note 52, at 4.

[339] *See, e.g., Letter from the President--War* ***Powers*** *Resolution*, OFF. PRESS SECRETARY, WHITE HOUSE (June 13, 2016), http://obamawhitehouse.archives.gov/the-press-office/2016/06/13/letter-president-war-***powers***-resolution [http://perma.cc/P4QA-SVK9].

[340] *See, e.g.*, Charlie Savage & Mark Landler, *White House Defends Continuing U.S. Role in Libya Operation*, N.Y. TIMES (June 15, 2011), http://www.nytimes.com/2011/06/16/us/politics/16powers.html [http://perma.cc/FSB9-PSS7] (discussing the report provided to Congress after assertion of WPR violation, in which State Department Legal Advisor Harold Koh interpreted the definition of "hostilities" to exclude the Libya conflict).

lawsuits would have the same effect. They would help tilt the political balance in favor of Congress, highlight ***executive*** malfeasance, and buttress norms of ***executive*** accountability in the appropriations space. [341]

[*2576] Moreover, if Appropriations Clause lawsuits are even partially successful, Congress could gain greater leverage against the President. For instance, suppose a district court decides an Appropriations Clause case in Congress's favor, but on appeal the decision is reversed. If the appeals court does not reverse on the merits, Congress would still have a favorable district court decision with which to confront the President--an opinion from a neutral party that Congress's view of the issue is correct. Alternatively, suppose that a court sides with Congress in an Appropriations Clause case but determines that an injunction would be inappropriate. Assuming that Article III case-or-controversy requirements were met, the court could still grant Congress a declaratory judgment. [342] This would not directly force the President to change course, but would strengthen Congress's hand in its political battle with the ***Executive***. And in either of these cases, if the President still refused to comply with Congress's appropriations decision, the lawsuits and any court determinations could become evidence of separation-of-***powers*** violations that Congress could rely on in impeachment proceedings. The first article of impeachment against Andrew Johnson, for instance, accused him of violating his constitutional duty to see that the laws be faithfully executed because he dismissed his Secretary of War without senatorial authorization in violation of the Tenure of Office Act. [343] A judicial declaration that a President has violated an appropriations law would provide a stronger argument for impeachment based on a Take Care Clause infraction than did Congress's say-so alone in the Johnson impeachment trial.

---

[341] One might wonder why the President, having defied Congress's will in spending unappropriated funds, would not similarly defy the judiciary. But the President's relationships with the two branches are different in this regard, both theoretically and practically. At a theoretical level, a President may spend funds that Congress believes it had not appropriated, not necessarily out of malevolence, but rather because the ***executive*** branch has a colorable legal argument that the President does in fact have the ***power*** to spend the money, based either on an interpretation of the appropriations statute or on a constitutional argument that Congress cannot tie its hands. *See, e.g.*, Maura Dolan, *Judge Refuses To Block Trump's Order To End Obamacare Subsidies*, L.A.TIMES (Oct. 25, 2017), http://www.latimes.com/local/lanow/la-me-ln-states-healthcare-lawsuit-20171024-story.html [http://perma.cc/K79W-XRU5] ("The Obama administration decided that the language of the law constituted a so-called permanent appropriation, which allowed it to make the payments without further congressional action . . . ."). If the courts decide the legal issue in Congress's favor, the President loses her main defense and will face both internal ethical pressure and external political pressure to comply. On a practical level, Presidents have nearly always complied with court orders in cases in which the President's legal interpretations clashed with those of Congress or another political branch official--even when the cases were both notable and controversial.*See, e.g.*, John P. MacKenzie, *Court Orders Nixon To Release Tapes*, WASH. POST (July 25, 1974), http://www.washingtonpost.com/politics/court-orders-nixon-to-yield-tapes-president-promises-to-comply-fully/2012/06/04/gJQAZSw0IV_story.html [http://perma.cc/SF69-SEGN] (noting that President Nixon promised to hand over Watergate tapes to an independent prosecutor after having claimed ***executive*** privilege);*President Bush and Japanese Prime Minister Koizumi Participate in a Joint Press Availability*, OFF. PRESS SECRETARY, WHITE HOUSE (June 29, 2006), http://georgewbush-whitehouse.archives.gov/news/releases/2006/06/20060629-3.html [http://perma.cc/7W69-XGK9] (showing that President Bush reacted to the decision inHamdan v. Rumsfeld, 548 U.S. 557 (2006), which held that military commissions were not authorized by Congress and thus could not try terrorists, by stating that he would work with Congress to authorize such commissions).

[342] *See* 28 U.S.C. § 2201 (2016); Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477, 513 (2010).

[343] *See The Impeachment of Andrew Johnson (1868)*, SENATE HIST. OFF., U.S. SENATE, http://www.senate.gov/artandhistory/history/common/briefing/Impeachment_Johnson.htm [http://perma.cc/5HAN-GSRT].

These signaling functions, while most directly useful in relation to the President, can also shape agency behavior. Agencies pay close attention to Congress's budgets and the priorities they express. Congress tends to provide lump-sum **[*2577]** payments in its budgets [344] and does not allow legislation in the text of an appropriations bill. [345] However, House and Senate rules require that Congress issue reports with descriptions of any policy changes in appropriations bills, [346] and agencies treat these reports as though they are legislation. [347] Agencies also tend to--but do not always--ask for permission from appropriations subcommittees before spending funds for purposes for which they were not appropriated. [348] Any decision Congress makes regarding appropriations, then, signals to agencies that Congress cares about the policy at issue and provides agencies with guidance about how funds are to be spent. [349] Agencies will pay close attention to any appropriation that Congress deems important enough to file suit in order to enforce. Recalcitrant cabinet secretaries, lacking the democratic mandate that helps inure the President to congressional criticism, may fall in line to avoid both the burden of the suits themselves and the inevitable political fallout that they now know will come if they maintain their existing interpretations of the appropriations.

Beyond the ***executive*** branch, Congress may wish to signal its priorities to the public. Members of Congress often act with an eye toward re-election, and the political fortunes of both parties and individual members hinge on the signals they send to the electorate about their activities. [350] Congress's appropriations decisions indicate its policy priorities; members must both appropriate consistently with the priorities on which they ran and show the public that they did so. [351] Successful lawsuits do both of these things. Even unsuccessful lawsuits, however, would signal to the public that legislators are fighting for the same policies the majority party promised it would enact. This is a particularly powerful form of what David Mayhew terms "position taking"--the phenomenon by which members of Congress are rewarded merely for taking positions. [352] Unsuccessful lawsuits would function much like the "message bills" that are commonly introduced, without much chance of passage, to signal a legislator's **[*2578]** priorities to her constituents. [353] A president's repeated violations of specific appropriations could become fodder for congressional and presidential campaigns alike. This makes it more likely that the substance of the appropriations restrictions themselves will be respected.

---

[344] CHAFETZ, *supra* note 8, at 71.

[345] Neal E. Devins, *Regulation of Government Agencies Through Limitation Riders*, 1987 DUKE L.J. 456, 458 n.12.

[346] *Id.*

[347] CHAFETZ, *supra* note 8, at 71-72.

[348] *Id.* at 72.

[349] *Id.*

[350] DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION, at xv, 5-6 (2d ed. 2004).

[351] *See* CHAFETZ, *supra* note 8, at 71.

[352] MAYHEW, *supra* note 350, at xv, 61.

[353] *See, e.g.*, Jennifer Steinhauer, *Congress's Look-Good Season: Republicans Pursue Bills To Show Voters*, N.Y. TIMES (July 9, 2016), http://www.nytimes.com/2016/07/10/us/politics/congresss-republicans-pursue-bills.html [http://perma.cc/95J9-XL5H].

Finally, Congress can send internal signals through Appropriations Clause lawsuits. The decision to engage in a series of lawsuits would inevitably affect how individual members approach the appropriations process. The suits would likely raise the profile of legislators who introduced the riders involved, and perhaps of the members who sponsored the riders or pushed to file the cases. Legislators may therefore be tempted to make policy through the appropriations process to a greater degree than they currently do. And if enough individual members start paying attention to the appropriations process as a way to make ***national security*** policy, they may see the benefit to banding together--which could lead to collective efforts by Congress to vindicate its institutional efforts in this area. In all of these ways, Appropriations Clause lawsuits could be an effective political tool for Congress to signal its positions to the ***Executive***, the people, and its own members.

C. Preventing an Assumption of Acquiescence

Third, and relatedly, even unsuccessful suits would serve a broader separation-of-***powers*** goal: combating the inference of congressional acquiescence to the accretion of ***executive power***. In his *Youngstown* concurrence, Justice Frankfurter explained the significance of historical gloss in the ***national security*** context, positing that "a systematic, unbroken, ***executive*** practice, long pursued to the knowledge of the Congress and never before questioned . . . may be treated as a gloss on '***executive Power***' vested in the President." [354] Historical practice remains an important factor in separation-of-***powers*** jurisprudence. [355] In *NLRB v. Noel Canning*, the Court interpreted the Recess Appointments Clause as conferring more ***executive power*** based in part on the Senate's history of confirming **[*2579]** presidential appointments in certain circumstances. [356] The Court took the same tack the next year for the recognition ***power*** in *Zivotofsky*. [357]

Courts could infer similar legislative acquiescence if Presidents ignore appropriations restrictions without any congressional response. To a judicial observer, congressional inaction in the face of ***executive*** overstepping could suggest that Congress approved of the transgressions. [358] A practice of congressional resolutions to pursue Appropriations Clause lawsuits--even if such lawsuits will not obtain success on the merits--would strongly combat the appearance of congressional acquiescence in ***executive*** appropriations misconduct. Narrowed appropriations could set the stage for a challenge by either legislators or a plaintiff with less significant justiciability concerns. When a case later arises in which courts can adjudicate the constitutionality of ***executive national security*** misappropriations, Congress's strongest-intended check will not fall victim to the courts' assumptions about what Congress might think of the President's actions.

Overall, through encouraging more careful appropriations ex ante, recalibrating the political calculus, and combatting any inference of acquiescence, Congress would restore some of its constitutional ***power*** over ***national security*** appropriations by the mere threat of Appropriations Clause litigation, even if a suit never reaches the merits. All of these would also be valuable in the event that justiciability doctrine changes to

---

354 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610-11 (1952) (Frankfurter, J., concurring).

355 NLRB v. Noel Canning, 134 S. Ct. 2550, 2559 (2014); *see also* Dames & Moore v. Regan, 453 U.S. 654, 676-83 (1981) (holding that, although Congress had not authorized President Carter to dismiss certain claims against Iran in the wake of the Iranian hostage crisis, prior congressional acquiescence rendered the actions constitutional).

356 134 S. Ct. at 2559, 2561-62, 2567, 2570-73.

357 Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076, 2091 (2015).

358 *Cf*. Burns v. United States, 501 U.S. 129, 136 (1991) ("In some cases, Congress intends silence to rule out a particular statutory application, while in others Congress' silence signifies merely an expectation that nothing more need be said in order to effectuate the relevant legislative objective.").

permit more latitude in legislator-initiated suits, or if a third party that clears the jurisdictional hurdles emerges.

VI. THE CASE AGAINST THE CLAUSE: RESPONDING TO THE MAIN CRITIQUES OF THIS CONGRESSIONAL STRATEGY

Given the historical interest that members of Congress have shown in pursuing ***national security*** lawsuits, and the model presented in *Burwell*, it is possible that courts will face more Appropriations Clause ***national security*** litigation in the future. Congress's use of this tool can be criticized on grounds of its wisdom, effectiveness, and appeal to partisanship. But ultimately these challenges fail to grasp the extent of the problem posed by the modern imbalance in the separation of ***powers***, and the targeted nature of the solution that Appropriations Clause litigation provides. Overall, the use of such lawsuits by Congress could **[*2580]** serve as an effective aid in recalibrating the imbalance of ***power*** and asserting its constitutional role in war making and ***national security***.

First, the specter of the robed, faceless, unelected judge ordering the President to withdraw troops from combat evokes, for many, a deep-seated discomfort. The traditional critique of judicial involvement in the war ***powers*** context resembles the arguments for applying the political question doctrine: judges lack the competence [359] to analyze the relevant facts [360] and decide what are essentially policy questions, [361] particularly where ***national security*** is at stake. [362]

These arguments against judicial involvement in foreign affairs and ***national security*** have been heavily criticized, [363] and are particularly inapplicable in the context of Appropriations Clause litigation. Judges have historically been involved in questions of ***national security***, [364] the separation of ***powers***, [365] and the Appropriations Clause. [366] The relevant factual questions are well within judicial competence; they require courts to answer whether Congress appropriated funds, and whether the President spent funds in violation of those restrictions. Deciding an appropriations challenge would not be tantamount to making policy: Congress made its policy determination by choosing to restrict funding, but the courts are needed to prevent unconstitutional actions in contravention of that policy.

---

[359] FISHER, *supra* note 2, at 303.

[360] THOMAS M. FRANCK, POLITICAL QUESTIONS/JUDICIAL ANSWERS: DOES THE RULE OF LAW APPLY TO FOREIGN AFFAIRS? 46-48 (1992).

[361] *Id.* at 48-50.

[362] *Id.* at 50-58.

[363] *See* Koh, *supra* note 160, at 122-25.

[364] KOH, *supra* note 5, at 220; *see also supra* Section III.A (arguing that it is possible that Congress could bring an Appropriations Clause claim).

[365] *See, e.g.*, Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076 (2015); NLRB. v. Noel Canning, 134 S. Ct. 2550 (2014); INS v. Chadha, 462 U.S. 919 (1983); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[366] UAWv. Donovan, 746 F.2d 855, 859-63 (D.C. Cir. 1984); Ramirez de Arellano v. Weinberger, 745 F.2d 1500, 1510-11 (D.C. Cir. 1984) (en banc), *vacated and remanded*, 471 U.S. 1113 (1985); City of Los Angeles v. Adams, 556 F.2d 40 (D.C. Cir. 1977); Stith, *supra* note 23, at 1386-87 & n.213 (citing TVA v. Hill, 437 U.S. 153 (1977)).

Arguments against judicial involvement in ***national security*** appropriations disputes rely heavily on the status quo, equating judicial abstention with neutrality and judicial involvement with activism and bias. But neutrality is not necessarily **[*2581]** neutral. Judicial abdication in these questions heavily favors the ***Executive***. [367] To insist that courts stay out of these disputes is to argue that Presidents should always have the last say, unless Congress pursues impeachment. But this position is entirely inconsistent with Congress's constitutional authority over appropriations and war making, as envisioned by the Framers. The ability to keep leashed the dog of war was intended to be one of Congress's most effective checks on unbridled ***executive*** war making. To decline to adjudicate these disputes would be tantamount to cutting the leash.

Second, critics of ***national security*** appropriations litigation may contend that if a single house of Congress had standing to sue the President for any alleged appropriations misstep, these suits would be too easy to institute, resulting in "congressional end-runs around the legislative process and threaten[ing] to involve the courts in virtually every political dispute." [368] Because it is easier to get a majority of one house to vote to bring a lawsuit than to get a veto-proof two-thirds majority in each house to pass or repeal a law over a presidential veto, these suits might function as a bad faith means of congressional opposition.

Ultimately, however, Appropriations Clause suits are unlikely to be a frequent recourse. First, floods of litigation have not accompanied at least some past expansions of legislative standing, despite similarly calamitous predictions. [369] Second, Appropriations Clause lawsuits are not "end-runs around the legislative process" in the traditional sense because they already involve a completed legislative process--the appropriations bill at issue has been passed, and congressional plaintiffs can only seek judicial redress of its unconstitutional violation. Third, appropriations challenges are not "too easy" to bring. Individual members would not be able to seek redress of the institutional injury without authorization fromat least a majority of one house of Congress. Either Congress would have to pass ex ante framework legislation authorizing individual members to bring appropriations challenges, or individual members would need to seek authorization via resolution for each lawsuit. Similarly, congressional plaintiffs would need either to point to an explicit restriction that was violated or to have **[*2582]** previously restructured ***national security*** appropriations in order to argue in the future that spending for a certain activity did not fit within narrow appropriations categories. The legislative activity that this would require would likely weed out frivolous claims. [370]

But even if appropriations litigation only occurs in the most extreme circumstances--when a President engages in ***national security*** decisions so objectionable that her own party is willing to oppose it--that is enough of an application for these lawsuits to be an effective and useful tool. Even in these limited circumstances, Appropriations Clause litigation would vindicate the constitutional prerogatives of Congress

---

[367] KOH, *supra* note 5, at 219 ("[V]irtually all of the cases on foreign affairs allegedly decided under the [political question] 'doctrine' actually involved judicial determinations upholding ***executive*** decisions on the merits." (citing Louis Henkin, *Is There a "Political Question" Doctrine*?, 85 YALE L.J. 597, 606 (1976)); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1313 (1988) ("[T]he Court has condoned ***executive*** initiatives in foreign affairs by refusing to hear challenges to the President's authority.").

[368] Meyer, *supra* note 53, at 67 (discussing the possibility of congressional lawsuits generally to help correct the imbalance in constitutional ***powers***).

[369] *Id.* at 115 ("No flood of litigation followed *Coleman v. Miller*, despite Justice Frankfurter's similarly expressed fear . . . .").

[370] *See supra* Section I.B.

as an institution. And correcting the institutional imbalance of ***power*** that has developed between the political branches, contrary to constitutional design, is precisely the goal that the Appropriations Clause can help to serve.

A final critique of Congress's use of appropriations litigation is that it will limit presidential discretion in the conduct of ***national security***. [371] If Congress only seeks to bring appropriations litigation in response to violations of explicit restrictions, presidential flexibility in ***national security*** spending would continue unaffected. However, if Congress recognizes the usefulness of such litigation, it could potentially remove presidential spending discretion and narrowly appropriate in order to bring appropriations litigation for illegally transferring funds between the narrow appropriations categories. In this scenario, Congress would have limited presidential discretion, and--critics would argue--removed the President's ability to respond quickly and flexibly to a ***national security*** crisis.

However, this argument ignores the history of appropriations and presidential emergency action. In the past, when the President was faced with an emergency, she was expected to convene Congress immediately to appropriate funds, or to take on the risk of spending unappropriated funds and asking Congress to sanction the act as soon as possible. [372] The President would still have that option if Congress returned to a structure of narrow, specific ***national security*** appropriations. In the case of a true emergency, the President can respond; but she assumes the risk that Congress will not affirmatively sanction the expenditure **[*2583]** after the fact. [373] This system properly places the burden on the President, because the Constitution intends that the President should try to avoid those risks by seeking political approval and appropriations *before* acting.

To the extent some effects of appropriations litigation may be undesirable, it is simply the price we must pay "for our system of checks and balances." [374] Although the price sometimes seems "exorbitant to many," on balance it is desirable to fortify legislative ***powers*** against ***executive*** encroachment, because though a "kindly President" may overstep the separation of ***powers*** today, there is no telling how "another President might use the same ***power***" tomorrow. [375]

CONCLUSION

Over the past four decades, members of Congress have attempted to use the judiciary to vindicate Congress's constitutional war ***powers***. Though this series of lawsuits has failed repeatedly to reach the merits, Appropriations Clause litigation offers hope for those seeking to help Congress reclaim its constitutional role in ***national security***. By pursuing lawsuits authorized by a majority of a house of Congress claiming that the President spent unappropriated funds in violation of the Appropriations Clause,

---

[371] Which of course assumes that presidential discretion is a good thing. *See, e.g.*, BANKS & RAVEN-HANSEN, *supra* note 15, at 180 (opining that discretionary spending authority "gives the president intended and, in our view, often desirable flexibility").

[372] *See supra* Section I.A. The War ***Powers*** Act also recognized the existence of true emergencies for which pre-consultation would not be possible. 50 U.S.C. § 1542 (2012) ("The President *in every possible instance* shall consult with Congress before introducing United States Armed Forces into hostilities . . . ." (emphasis added)).

[373] Of course, in a true emergency Congress is unlikely to sanction the President with a lawsuit for failing to seek pre-approval, because this would be politically inexpedient.

[374] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 633 (Douglas, J., concurring).

[375] Id. at 633-34.

congressional plaintiffs could have a greater chance of reaching and succeeding on the merits in ***national security*** disputes.

The biggest hurdle for ***national security*** appropriations litigation is getting to the merits. Historically, lawsuits brought by members of Congress generally, [376] ***national security*** lawsuits against the ***Executive***, [377] and lawsuits regarding "***executive*** compliance with appropriations limitations" [378] have all had a difficult time reaching resolution the merits. Once one of these suits reaches the merits, however, it stands a fair chance of success, if preceded by proper legislative action. In order to make a claim for violation of an explicit denial of appropriations, Congress must have passed such a restriction. And in order to proceed on a theory of violation of narrow appropriations, Congress must limit ***executive*** **[*2584]** discretion in ***national security*** expenditures and appropriate in smaller buckets. If Congress can establish the factual predicate--that the President spent unappropriated funds--it must succeed in arguing that its constitutional authority over appropriations trumps the President's constitutional authority over the ***national security*** object in dispute. Given the strong ***original*** understanding of the appropriations ***power***, [379] and the scholarly consensus about its breadth, [380] courts should rule for congressional plaintiffs in Appropriations Clause standoffs, as long as the appropriation restriction at issue did not usurp the President's Commander-in-Chief authority. [381] Should Congress include restrictions under its authority to declare war--for example, those that prevent the use of funds to expand the theatre of an existing conflict--courts should find that the legislation abided constitutional boundaries.

Judicial review of Appropriations Clause violations in the ***national security*** context would help reinforce both Congress's purse ***power*** and its war ***power***. A sensible use of the judicial forum could help the courts meet the goal set by Justice Breyer: to "assure constitutional accountability, even of the president and even in time of war or national emergency." [382] A more robust role for the courts in this form of separation-of-***powers*** dispute could result in a much-needed recalibration of the constitutional balance of ***powers*** in the ***national security*** sphere.

Yale Law Journal
Copyright (c) 2018 The Yale Law Journal Company, Inc.
The Yale Law Journal

End of Document

---

[376] Meyer, *supra* note 53, at 75 ("The courts have reached the merits in only eight of the more than forty lawsuits in which members of Congress were plaintiffs.").

[377] *See* FISHER, *supra* note 2, at 302.

[378] Stith, *supra* note 23, at 1387 ("Often, however, when faced with an issue of ***executive*** compliance with appropriations limitations, courts have declined to decide cases on the merits.").

[379] *See supra* Section I.A.

[380] *See supra* notes 9493-97 and accompanying text.

[381] *Cf.* NANCY STAUDT, THE JUDICIAL POWE ROF THE PURSE 67-68 (2011) (arguing that, where the President supports increased ***national security*** spending and military operations and Congress opposes it, "judges are likely to prioritize congressional views in this particular context" when making decisions with fiscal consequences).

[382] STEPHEN G. BREYER, MAKING OUR DEMOCRACY WORK: A JUDGE'S VIEW 193 (2011).

ARTICLE: Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats

2016

Reporter
7 Harv. Nat'l Sec. J. 391 *
Length: 10741 words
Author: John P. Carlin *

* Assistant Attorney General for ***National Security***, United States Department of Justice. I would like to thank David Forscey, Chloe Goodwin, Megan Henry, Sarah Howard, Allison Kempf, Alan Rozenshtein, Paul Schied, Yishai Schwartz, and Joshua Silverstein for their help in preparing this Article. I would also like to thank Josh Goldfoot, Chris Hardee, Adam Hickey, Alex Iftimie, James Melendres, Anita Singh, Brad Wiegmann, and several other individuals both inside and outside the government for their comments and assistance. This material has been reviewed by the Department of Justice to prevent the disclosure of classified information.

Copyright [c] 2016 by the Presidents and Fellows of Harvard College and John P. Carlin

Text

[*393] Introduction

The United States faces an inflection point when it comes to the Internet's effect on daily life. What has enriched our economy and quality of life for the past several decades may start to hurt us more than help us, unless we confront its ***cybersecurity*** challenges. [1] Waves of network intrusions--increasing in number, sophistication, and severity--have hit American companies and the U.S. government. In 2012, former CIA Director and Defense Secretary Leon Panetta described the nation's ***cybersecurity*** weaknesses as presenting a "pre-9/11 moment." [2] And in July 2014, the 9/11 Commission itself warned: "We are at

---

[1] For the purposes of this Article, "***cybersecurity***" means the protection of "computers, networks, programs and data from unintended or unauthorized access, change or destruction." "Cyberspace" refers to the "interdependent network of information technology infrastructures[] that includes the Internet, telecommunications networks, computer systems and embedded processors and controllers." *What is* ***Cyber Security***?, UNIV. OF MD. UNIV. COLL., http://www.umuc.edu/***cybersecurity***/about/***cybersecurity***-basics.cfm. Importantly, ***cybersecurity*** extends to the protection of devices that are connected to the Internet--whether large-scale critical infrastructure or consumer devices (e.g., the emerging "Internet of Things"). More generally, the word or prefix "***cyber***" broadly refers to the domain of activity that arises from the close integration of computers, and in particular the Internet, into our society. The term has its detractors, who prefer more specific terms like "online" or "network." Nevertheless, the term is used here to capture, in one word, otherwise disperse subjects that are the greatest concern in governance.

[2] Leon E. Panetta, U.S. Sec'y of Def., Remarks by Secretary Panetta on ***Cybersecurity*** to the Business Executives for ***National Security***, New York City (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

September 10th levels in terms of ***cyber*** preparedness." [3] Following that ominous prediction, in a span of less than two years, the United States was besieged by intrusions originating from around the globe. There was no single target, and no common perpetrator. Our adversaries stated or demonstrated that they hacked on behalf of China, North Korea, Syria, Iran, and many others. They stole sensitive information from government databases, damaged and destroyed private companies' computer systems, and--in a new twist--even targeted individuals' personally identifiable information to benefit terrorist organizations. The list of victims is broad and varied--the private sector, the government, and individual citizens. The past two years have publicly demonstrated the extent of the threat.

Former Federal Bureau of Investigation (FBI) Director Robert Mueller once offered the following analogy to describe our growing ***cyber*** vulnerabilities:

> In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles. The Romans built these roads to access the vast areas they had conquered. But, in the **[*394]** end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates. [4]

Like the Roman roads, the Internet connects us to the world. Empowered by advances in technology like cheap storage, increased bandwidth, miniaturized processors, and cloud architecture, we've extended Internet connectivity throughout our lives. But this expansion carries a risk not fully accounted for. Increased connectivity makes our critical infrastructure--water, electricity, communications, banking--and our most private information more vulnerable. We invested an enormous amount over the past few decades to digitize our lives. But we made these investments while systematically underestimating risks to our digital ***security***. If we don't secure our Internet connectivity, what has been an important driver of prosperity and strength for the past twenty years could have disastrous effects in the next twenty.

To meet this challenge, the U.S. government has changed its approach to disrupting ***national security cyber*** threats. One element of its new strategy involves implementing and institutionalizing a "whole-of-government" approach. No one agency can beat the threat. Instead, success requires drawing upon each agency's unique expertise, resources, and legal authorities, and using whichever tool or combination of tools will be most effective in disrupting a particular threat. At times, that may mean economic sanctions from the Treasury Department, proceedings initiated by the Office of the U.S. Trade Representative, and ***cyber*** defense operations from the Defense Department. At other times, it might mean information sharing coordinated by the Department of Homeland ***Security***, diplomatic pressure from the State Department, ***intelligence*** operations from the U.S. ***Intelligence*** Community (IC), [5] and prosecution and other legal

---

[3] BIPARTISAN POLICY CTR., REFLECTIONS ON THE TENTH ANNIVERSARY OF THE 9/11 COMMISSION REPORT (July 2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf.

[4] Robert S. Mueller, Dir., Fed. Bureau of Investigation, Speech at Penn State Forum Speaker Series State College, Pennsylvania, The FBI: Stopping Real Enemies at the Virtual Gates (Nov 6, 2007), https://www.fbi.gov/news/speeches/the-fbi-stopping-real-enemies-at-the-virtual-gates.

[5] The IC is "a coalition of 17 agencies and organizations . . . within the Executive Branch that work both independently and collaboratively to gather and analyze the ***intelligence*** necessary to conduct foreign relations and ***national security*** activities." OFFICE OF THE DIR. OF NAT'L ***INTELLIGENCE***, http://www.dni.gov/index.php. It consists of: Air Force ***Intelligence***, Army ***Intelligence***, Central ***Intelligence*** Agency, Coast Guard ***Intelligence***, Defense ***Intelligence*** Agency, Department of Energy, Department of Homeland ***Security***, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps ***Intelligence***, National Geospatial-

action from the Justice Department. And in many instances, it will mean a coordinated application of several capabilities from the U.S. government's menu of options.

The United States' approach to combating Chinese theft of sensitive U.S.-company business information and trade secrets--activity that former ***National Security*** Agency Director Keith Alexander described as the "greatest transfer of **[*395]** wealth in history" [6] --illustrates the power of this coordinated approach. In May 2014, after an unprecedented investigation spanning several years, a federal grand jury indicted [7] five uniformed members of the Chinese military on charges of hacking and conducting economic espionage against large U.S. nuclear-power, metal, and solar-energy companies. The 48-page indictment describes numerous, specific instances where officers of the People's Liberation Army (PLA) hacked into the computer systems of American companies to steal trade secrets and sensitive, internal communications that could be used for economic gain by Chinese companies. The recipient companies could use the stolen information against the victims in competition, negotiation, and litigation. [8]

This landmark case was the first prosecution of official state actors for hacking. [9] But the indictment was not pursued in isolation; nor was it seen as an end in and of itself. Rather, the investigation and prosecution of the PLA members were pieces of a larger deterrence strategy. In spring 2015, the President issued an executive order authorizing sanctions against companies engaging in malicious ***cyber*** activity. [10] At the same time, the government was advocating diplomatically for basic international norms in cyberspace.

It appears that these coordinated efforts are starting to establish new norms in cyberspace. In September 2015, President Obama and Chinese President Xi Jinping affirmed that neither country's government will conduct or knowingly support ***cyber***-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. [11] Although we don't know the extent to which China will honor this commitment, the fact that the commitment was made is itself significant, as is the fact that at the November 2015 G20 Summit

---

Intelligence Agency, National Reconnaissance Office, ***National Security*** Agency, Navy ***Intelligence***, and the Office of the Director of National ***Intelligence***.*Id.*

[6] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History*," FOREIGN POLICY (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrimeconstitutes-the-greatest-transfer-of-wealth-in-history/.

[7] Throughout this Article, I refer to indictments and other criminal complaints. It is important to note that an indictment contains allegations that a defendant has committed a crime, and every defendant is presumed to be innocent until proven guilty in court.

[8] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for ***Cyber*** Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-***cyber***-espionage-against-us-corporations-and-labor [hereinafter PLA Indictment Summary]. Federal prosecutors in the Western District of Pennsylvania, where the indictment was returned, deserve special mention. The U.S. Attorney's Office for the Western District of Pennsylvania, led by U.S. Attorney David Hickton, has been at the forefront of pursuing ***cyber***-related federal prosecutions, despite the challenges that such cases pose due to their novelty, length, and cost.

[9] *Id.*

[10] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015)

[11] *See* Press Release, White House, FACT SHEET: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheetpresident-xi-jinpings-state-visit-united-states.

in Turkey, leaders representing the twenty largest economies in the world **[*396]** agreed to norms related to acceptable behavior in cyberspace. [12] As President Obama has noted, the Internet can sometimes seem like the "Wild Wild West." [13] But we are beginning to bring law and order to the Internet through concrete actions designed to ensure there are consequences for impermissible or unlawful behavior in cyberspace.

A whole-of-government approach is critical to success in disrupting ***national security*** ***cyber*** threats. But given the complexity of the threats we face, no strategy, regardless of the number of agencies involved or the breadth of tools available, would be complete without coordination with the private sector. In an increasingly flattened and connected world, the threat can easily move and change--but one constant is that private entities remain on the front lines of this fight. Thus, a second element of the United States' new approach involves deeper partnerships with the private sector.

This Article explains how ***national security*** investigators and lawyers in the Department of Justice (DOJ) play a crucial role in this new approach. As practiced at DOJ, ***national security*** law goes beyond the use of one set of tools or body of law. It is cross-disciplinary--encompassing a practical, problem-solving approach that uses all available tools, and draws upon all available partners, in a strategic, ***intelligence***-driven, and threat-based way to keep America safe. As former Acting Assistant Attorney General (AAG) for ***National Security*** Todd Hinnen has noted, "[n]ational ***security*** investigations seek to harness and coordinate the authorities and capabilities of all members of the ***national security*** community, state and local law enforcement, and foreign law enforcement and ***intelligence*** partners," [14] and "may result in a wide variety of ***national security*** activity, including . . . arrest and prosecution of perpetrators, imposition of economic sanctions, diplomatic overtures to foreign governments, and actions undertaken by U.S. ***intelligence*** services or armed forces overseas." [15]

Key to almost any of these responses is attribution. Attribution is the ability to confidently say who did it: which country, government agency, group, or even individual is responsible for a ***cyber*** intrusion or attack. To respond to ***cyber*** activity, you must know who is responsible, and what makes them tick. Defense, deterrence, and disruption all require an understanding of the adversary. [16] Government lawyers, agents, analysts, computer scientists, and other **[*397]** ***national security*** investigators are particularly good at developing the building blocks of attribution--they have expertise honed in criminal investigations and carry a host of legal authorities that allow them to investigate and gather information.

Although attribution is a simple idea, doing so on the Internet is very complex. The Internet's architecture allows hackers to route their activities through a global network of computers, almost all of which are owned

---

[12] G20 LEADERS' COMMUNIQUé, ANTALYA SUMMIT 6 (2015), http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[13] Nicole Perlroth & David E. Sanger, *Obama Calls for New Cooperation to Wrangle the "Wild West" Internet*, N.Y. TIMES (Feb. 13, 2015), http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-***security***.html.

[14] Todd Hinnen, ***National Security*** *Investigations, in* ***NATIONAL SECURITY*** LAW IN THE NEWS 215, 225 (Paul Rosenzweig et al. eds., 2012).

[15] *Id.* at 215-16.

[16] *See, e.g.*, David D. Clark & Susan Landau, *Untangling Attribution, in* COMM. ON DETERRING CYBERATTACKS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 25 (2010).

and operated by a variety of private actors. In addition, knowing which specific computer or network caused the malicious activity doesn't necessarily tell you which person or organization ordered, carried out, or supported the hack.

But attribution is still possible. DOJ, including the Federal Bureau of Investigation (FBI) and other law enforcement agencies, and with support from the IC, has unique expertise and legal authorities it can use to attribute ***cyber*** activities to their source. We can then take steps based on that attribution--including but not limited to prosecuting those responsible--to help us fight ***cyber*** threats. Each of these steps may seem small, but incrementally they can help us turn the tide.

This Article proceeds in three parts. Part I describes the ***cyber*** threats we face and emphasizes that any long-term solution must include deterrence and disruption. Part II explains why DOJ is well-placed to attribute network intrusions, and how it goes about doing so. Part III lays out the tools--within DOJ, across the federal government, and in the private sector--that rely on attribution to defend against, disrupt, and deter ***cyber*** threats. Throughout, this Article attempts to give concrete details and examples. But the need to protect sensitive sources and methods--in particular the means by which the government attributes ***cyber*** activity--limits what can be publicly described.

Before proceeding, it's important to emphasize that we are at the very beginning of the effort to confront ***national security cyber*** threats. All of the organizational and legal innovations discussed below--for example, increased ***intelligence*** coordination and the use of prosecutions, sanctions, and other legal tools to counter ***cyber*** threats--are evolving. The number of successful operations is still modest, especially given the size of the problem. And although we're moving in the right direction, we need to move faster.

We might need to modify or abandon some of the approaches if they prove unworkable, unscalable, or ineffective. Tools and techniques we haven't even thought of may ultimately take center stage. We welcome criticism and suggestions--indeed, encouraging this conversation is one of the main purposes behind this Article.

[*398] I. The ***Cyber*** Threat and the Need for Deterrence

The United States is under constant attack online. Every day, a wide range of actors try to hack government agencies, non-government organizations (NGOs), non-profits, and private companies. Some seek proprietary information and trade secrets. Others hunt for classified military documents and ***intelligence*** files, or information concerning NGOs or dissident activities. And still others want control over our infrastructure for disruptive, destructive, or even deadly ends. The culprits range from lone hackers in the United States, to organized criminal syndicates, to foreign military or ***intelligence*** officers and their proxies, to terrorists acting from terminals around the world. The vast majority fail, but too many still succeed.

Many of these activities--because of their motive, origin, or objective--threaten ***national security*** or public safety. For example, in addition to data loss, litigation risk, and reputational damage from ***cyber*** incidents, private sector companies now also confront the possibility of attacks that could destroy entire networks, threaten the viability of businesses, and even cause physical damage or loss of life.

To understand how we arrived at this troubling state of affairs, it is helpful to consider *how* ***cyber*** hacks operate, *who* perpetrates them, and *why* they're targeted at us.

A. *Means of Intrusion and Attack*

Hacking often begins with software vulnerabilities. Every time we access the Internet--whether it is to visit websites, check email, or use smartphone apps--we unwittingly expose ourselves to ***cyber*** threats. That's because software design prioritizes functionality. Developers often pay insufficient attention to ***security***

concerns, so most programs suffer from vulnerabilities that an intruder can exploit to get the software to crash or act in unexpected ways. That in turn can give intruders access to information or other programs, which they can use, for example, to install malware (software that is malicious by design). With full or even partial control over the system, malware can steal or delete information and target other computers. [17] Of course, when developers discover vulnerabilities for software, they usually distribute free patches. But users often fail to install patches, either because they're not aware of them or because installation is a resource-intensive hassle. According to one bulletin from the Department of Homeland ***Security***, "[c]yber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations. As many as 85 **[*399]** percent of targeted attacks are preventable." [18] The bulletin goes on to list "the 30 most commonly exploited vulnerabilities used in these attacks." [19] Patches exist for all of those vulnerabilities; for some, patches have existed for nearly eight years. [20]

Widespread software vulnerabilities enable industrial-scale hacking. For example, we face a proliferation of "botnets"--networks of thousands or even millions of malware-infected computers controlled by botnet "herders" for illicit uses, including attacking other systems. [21] Botnets are often responsible for distributed denial-of-service (DDoS) attacks, in which massive groups of computers simultaneously try accessing a website to overwhelm its servers and cause them to crash. One ***security*** research firm reported that, in the fourth quarter of 2014, such attacks increased by an annual 57% compared to the previous year. [22] Although DDoS attacks typically neither destroy computer systems nor degrade stored data, they can disrupt government services or make it impossible for companies to interact with their customers. DDoS attacks can have devastating economic effects, [23] and botnet herders have tried to extort large sums from companies by threatening DDoS attacks. [24]

---

[17] NAT'L ***SEC.*** AGENCY/CENT. ***SEC.*** SERV., DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE (2015), https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf.

[18] *Alert (TA15-119A): Top 30 Targeted High Risk Vulnerabilities*, U.S. COMPUT. EMERGENCY READINESS TEAM (Apr. 29, 2015), http://www.us-cert.gov/ncas/alerts/TA15-119A.

[19] *Id.*

[20] *See Microsoft* ***Security*** *Bulletin MS08-042--Important: Vulnerability in Microsoft Word Could Allow Remote Code Execution (955048)*, MICROSOFT (Aug. 12, 2008), https://technet.microsoft.com/library/***security***/ms08-042.

[21] "***Security*** researchers estimate that between 500,000 and one million computers worldwide are infected with GOZ, and that roughly 250,000 of those infected computers are active 'bots' in the GOZ network at any given time." Decl. of Special Agent Elliot Peterson in Supp. of Appl. for an Emergency TRO and Order to Show Cause re Preliminary Inj. at 3, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. June 2, 2014).

[22] Bill Brenner, *Q4 2014 State of the Internet--****Security*** *Report: Numbers*, AKAMAI (Jan. 29, 2015), https://blogs.akamai.com/2015/01/q4-2014-state-of-the-internet---***security***-report-somenumbers.html.

[23] *See, e.g.*, TIM MATTHEWS, INCAPSULA, INCAPSULA SURVEY: WHAT DDOS ATTACKS REALLY COST BUSINESSES 8 (2014), http://lp.incapsula.com/rs/incapsulainc/images/eBook%20%20DDoS%20Impact%20Survey.pdf (estimating that DDoS attacks can cost companies $ 40,000 every hour).

[24] *See* Liam Tung, *Giant DDoS Attacks Are Now Hitting 500Gbps as Criminals Flex Their Muscle*, ZDNET (Jan. 27, 2016), www.zdnet.com/article/giant-ddos-attacks-are-now-hitting-500gbps-as-criminals-flex-their-muscles/.

Botnets are good for more than just DDoS attacks. They also distribute malware. For example, an increasing number of organizations and individuals are targets of "ransomware"--malware through which hackers take control of and then threaten to delete or disseminate valuable files unless the victim pays a ransom (often in Bitcoin). [25] 2013 saw the spread of a new version of ransomware **[*400]** called CryptoLocker, which encrypts a user's files and demands a ransom of anywhere from $ 200 to $ 5,000. [26] In 2014, crypto-ransomware attacks increased by an astonishing 4,000%, and the total number of known ransomware attacks more than doubled. [27] More recently, we've seen a disturbing trend across the country of ransomware attacks aimed at hospitals. [28] By disrupting hospital operations, such attacks not only cut into hospitals' bottom line, but also put patient health at serious risk.

Hackers can also gain control over systems by preying on the human weaknesses of their users. Spearphishing schemes send customized, legitimate-looking emails to extract sensitive information or install malware. [29] Spear phishing is enabled by the expanding universe of personally identifiable information on the Internet. Skilled hackers can access public and private data--from tweets to medical records and everything in between. This information lets them craft messages that convince even the most ***cyber***-savvy among us to transfer money and divulge passwords and credit card numbers. Even military-grade encryption is worthless if you are tricked into giving your credentials to an overseas hacker pretending to be your employer's IT department. According to one industry ***security*** report, over 80% of companies with more than 2,500 employees were targets of spear-phishing attempts in 2014--a 40% increase over the

---

[25] *See* Lucian Constantin, *Ransomware that Demands Bitcoins Is Distributed by Malware that Steals Bitcoins*, PC WORLD (Mar. 25, 2014), http://www.pcworld.com/article/2111520/newbitcrypt-ransomware-variant-distributed-by-bitcoin-stealing-malware.html; Brian Krebs,*"Operation Tovar" Targets "Gameover" ZeuS Botnet, CryptoLocker Scourge*, KREBS ON ***SECURITY*** (June 2, 2014), http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameoverzeus-botnet-cryptolocker-scourge/ (reporting that the curators of the GameOver ZeuS botnet "loaned out sections of their botnet . . . for a variety of purposes," including infecting systems with CryptoLocker);*see generally Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/investigate/***cyber***/ransomware-brochure.

[26] James B. Comey, Dir., Fed. Bureau of Investigation, Statement Before the House Judiciary Committee (Oct. 22, 2015), https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureauof-investigation-7. In a perverse twist, CryptoLocker set up a "customer service" site to make paying the ransom easier.*See* Brian Krebs, *CryptoLocker Crew Ratchets Up the Ransom*, KREBS ON ***SECURITY*** (Nov. 6, 2013), http://krebsonsecurity.com/tag/cryptolocker-decryption-service/.

[27] SYMANTEC, INTERNET ***SECURITY*** THREAT REPORT 7 (2015), https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-***security***-threat-reportvolume-20-2015.pdf.

[28] *See, e.g.*, Alex Dobuzinskis & Jim Finkle, *California Hospital Makes Rare Admission of Hack*, *Ransom Payment*, REUTERS (Feb. 19, 2016), http://www.reuters.com/article/us-california-hospitalcyberattack-idUSKCN0VS05M; Brian Krebs,*Hospital Declares 'Internal State of Emergency' After Ransomware Infection*, KREBS ON ***SECURITY*** (Mar. 22, 2016), https://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/; Jim Finkle & Dustin Volz,*Washington's MedStar Computers Down for Second Day After Virus*, REUTERS (Mar. 29, 2016), http://www.reuters.com/article/us-usa-***cyber***-medstar-idUSKCN0WV1J7.

[29] *See Spear Phishing: Scam, Not Sport*, NORTON BY SYMANTEC, http://us.norton.com/spearphishing-scam-not-sport/article; *Spear Phishers Angling to Steal Your Financial Information*, FED. BUREAU OF INVESTIGATION (Apr. 1, 2009), https://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

prior year. [30] Spear phishing will only get more sophisticated as hackers **[*401]** improve their social-engineering techniques and steal even more of our personal data. [31]

B. *Threat Actors*

Although hacking is a skill that requires knowledge and experience, hackers don't need (and often don't have) formal training. Computer skills can be honed anywhere, using materials publicly available on the Internet, and the equipment needed to engage in malicious activity and evade detection is inexpensive and widely available. As a result, we face ***cyber*** threats driven by an array of groups--from Russian criminal syndicates, to Al-Qaeda and the so-called Islamic State of Iraq and the Levant (ISIL), to foreign ***intelligence*** services and their proxies. As scholars Benjamin Wittes and Gabriella Blum have noted, cyberspace is a world of distributed threats, easily available weapons, and universal vulnerability. [32] Reviewing the different actors we confront in cyberspace--especially terrorist groups and ***foreign powers***--and the disturbing and dangerous ways in which these threats are blending with one another, illustrates the troubling breadth of the ***cyber*** threat.

Today, many of the same terrorist organizations that have threatened our ***national security*** for years actively seek to attack America over the Internet. For example, in 2012 Al-Qaeda released a video comparing the vulnerabilities in computer network ***security*** to weak points in aviation ***security*** before 9/11. [33] The film called for "electronic jihad" against the United States. [34] James Clapper, the Director of National ***Intelligence*** (DNI), noted in his 2014 Worldwide Threat Assessment that "terrorist organizations have expressed interest in developing offensive ***cyber*** capabilities," in addition to their established expertise in using the **[*402]** Internet to recruit personnel, finance activities, and disseminate propaganda. [35] In 2015, he predicted that many of these groups would likely "continue to experiment with hacking, which could

---

[30] *See* SYMANTEC, *supra* note 27, at 7.

[31] *See* Phil Muncaster, *Spear Phishing to Get More Personal in 2015*, INFOSECURITY (Dec. 22, 2014), http://www.infosecurity-magazine.com/news/spear-phishing-to-get-more. Social engineering attacks "typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file." Nate Lord,*Social Engineering Attacks: Common Techniques and How to Prevent an Attack*, DIG. GUARDIAN (May 18, 2016), https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-preventattack.

[32] *See generally* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE (2015).

[33] *Senators Say Video Urging Electronic Jihad Underscores Need for* ***Cybersecurity*** *Standards*, U.S. SENATE COMM. ON HOMELAND ***SEC.*** AND GOVERNMENTAL AFF. (May 22, 2012), http://www.hsgac.senate.gov/media/majority-media/senators-say-video-urging-electronic-jihadunderscores-need-for-***cybersecurity***-standards.

[34] Jack Cloherty, *Virtual Terrorism: Al Qaeda Video Calls for "Electronic Jihad,"* ABC NEWS (May 22, 2012), http://abcnews.go.com/Politics/***cyber***-terrorism-al-qaeda-video-calls-electronicjihad/story?id=16407875.

[35] OFFICE OF THE DIR. OF NAT'L ***INTELLIGENCE***, WORLD WIDE THREAT ASSESSMENT OF THE U.S. ***INTELLIGENCE*** COMMUNITY 2 (2014), http://www.dni.gov/files/documents/***Intelligence***%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

serve as the foundation for developing more advanced capabilities." [36] This danger is exacerbated by the empowerment of terrorist sympathizers through social media messaging campaigns on behalf of groups such as ISIL. DNI Clapper suggested that such supporters could conduct small-scale online attacks on behalf of terrorist organizations, thereby enhancing the threat these groups pose to the United States. [37] While these groups might not possess powerful ***cyber*** capabilities today, there should be no doubt that they are actively working to acquire them.

Even absent terrorist attacks conducted *through* cyberspace, we have already seen how ***cyber*** and terror threats can blend in dangerous ways. As just one example demonstrating how ***cyber*** attacks can be used to facilitate real-world terrorist attacks in unexpected ways, in August 2015, ISIL-affiliated hackers publicly released the names, locations, phone numbers, and e-mail addresses of over 1,000 U.S. military and other government personnel for the purpose of encouraging terrorist attacks against them. In a first-of-its-kind case, DOJ charged Ardit Ferizi, who ultimately pled guilty, [38] with material support for providing this stolen information to ISIL. [39]

The other major category of ***national security cyber*** threat actors consists of states and their proxies. The IC has characterized China's history of economic espionage against the American private sector as an "advanced persistent threat." [40] China's military and ***intelligence*** services possess the sophistication and **[*403]** resources to hack systems using multiple vectors, surreptitiously establish footholds behind perimeter defenses, exfiltrate valuable information, and undermine critical network functions. [41] These are not merely theoretical capabilities--China has routinely used such tactics against the United States over an extended period of time, adapted to our responses, and progressively escalated its intrusions. [42]

---

[36] OFFICE OF THE DIR. OF NAT'L ***INTELLIGENCE***, WORLD WIDE THREAT ASSESSMENT OF THE U.S. ***INTELLIGENCE*** COMMUNITY 3 (2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [hereinafter ODNI WWTA 2015].

[37] *Id.*

[38] *See* Press Release, U.S. Dep't of Justice, ISIL-Linked Hacker Pleads Guilty to Providing Material Support (June 15, 2016), https://www.justice.gov/opa/pr/isil-linked-hacker-pleads-guiltyproviding-material-support.

[39] *See* Press Release, U.S. Dep't of Justice, ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges (Oct. 15, 2015), http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-uscharges; Complaint, United States v. Ferizi, No. 1:15-MJ-00515, 2015 WL 6126125, (E.D. Va. Oct. 6, 2015).

[40] *See* ODNI WWTA 2015, *supra* note 36, at 3 (naming Chinese economic espionage an "advanced persistent threat" and specifically describing a believed Chinese hack that resulted in stolen personally identifiable information on 4.5 million individuals from U.S. company Community Health Systems); OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 5 (2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (private sector specialists describe the "onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China" as "advanced persistent threats");*see also* NAT'L INST. OF STANDARDS & TECH., MANAGING INFORMATION ***SECURITY*** RISK: ORGANIZATION, MISSION, AND INFORMATION SYSTEM VIEW 8 (2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (defining "advanced persistent threat" as "a long-term pattern of targeted, sophisticated attacks").

[41] *See* ODNI WWTA 2015, *supra* note 36, at 2 (describing China as a nation with a "highly sophisticated" ***cyber*** program).

[42] *Id.* at 3.

Beyond China, the United States has also publicly identified other foreign nations that pose a ***cyber*** threat to American ***national security***. Iranian hackers who worked for computer ***security*** companies affiliated with the Iranian government, including the Islamic Revolutionary Guard Corps, [43] were publicly charged in March 2016 with perpetrating DDoS attacks on the U.S. financial sector in which 46 financial institutions were flooded with traffic over the course of 176 days. The attacks disrupted online services and prevented hundreds of thousands of Americans from accessing their bank accounts online. In all, these attacks cost victims tens of millions of dollars. One of these defendants was also charged with obtaining unauthorized access to the computer systems controlling the Bowman Dam in Rye, New York. [44] At the time of his alleged intrusion, the dam was undergoing maintenance and had been disconnected from the system. But under ordinary circumstances, the access would have enabled him to control water levels and flow rates. DNI Clapper also implicated Iranian actors in the February 2014 ***cyber*** attack on the Las Vegas Sands Casino. [45]

In late 2014, North Korea was also publicly named as a nation engaged in ***cyber*** intrusions. After a rigorous FBI investigation into the November 2014 attack against Sony Pictures Entertainment, described more fully below, the U.S. government announced that North Korea was responsible. [46] Only months later, President Barack Obama signed an executive order authorizing additional actions against the North Korean government in response to the cyberattack.

[*404] Finally, in early 2015, DNI Clapper testified before the Senate that Russia, among other states, has a "highly sophisticated ***cyber*** program" that could harm the United States through economic espionage and "reconnoitering and developing access to U.S. critical infrastructure systems." [47]

The list goes on. These are only the countries we have publicly called out for this behavior. There are many more.

C. *Motivations*

Economic espionage is a key driver of many of the data breaches and exfiltrations that have received front-page attention over the past several years. [48] While it is hard to accurately determine losses, the FBI has estimated that in fiscal year 2012 economic espionage and the theft of trade secrets cost the American

---

[43] The Islamic Revolutionary Guard Corps is one of several entities within the Iranian government responsible for Iranian ***intelligence***.

[44] Press Release, U.S. Dep't of Justice, U.S. Atty's Office, S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign of ***Cyber*** Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorneyannounces-charges-against-seven-iranians-conducting-coordinated.

[45] ODNI WWTA 2015, *supra* note 36, at 3.

[46] *See* Press Release, Fed. Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[47] ODNI WWTA 2015, *supra* note 36, at 2.

[48] In 2011, the Office of the National Counterintelligence Executive issued a landmark report in which the IC directly identified China, Russia, and other countries as engaged in widespread economic espionage and theft of trade secrets against the United States. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE (2011), https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

economy over $ 19 billion. [49] The Office of the National Counterintelligence Executive [50] has estimated that losses from economic espionage could be orders of magnitude higher. [51] When foreign states steal intellectual property and business strategies from U.S. companies, those firms not only lose valuable proprietary information, they also face regulatory costs, litigation risk, reputational damage, customer or investor flight, and greater competition from companies that unfairly benefit from receiving the stolen information. The consequences of economic espionage are measured not only in terms of the substantial cumulative cost to U.S. companies, but also in the diminution of the competitive advantages of the American economy as a whole. [52]

[*405] Foreign adversaries also hack computer networks for counterintelligence purposes. This is a particular threat for federal employees and contractors, who by necessity must disclose personal information to their government. Malicious actors might use this information to blackmail, extort, and even recruit Americans to serve their ends. The hacks on personnel databases maintained by the Office of Personnel and Management crystalized this threat. Attackers stole dossiers of professional, financial, medical, and personal details for 21.5 million people, some of whom were working at the highest levels of our government. Almost two million people included in this dragnet were the partners and family members of those undergoing background investigations. Many private sector companies have also been targeted for the large volumes of personally identifiable information they maintain, the value of which extends beyond that of identity theft for criminal profit. [53]

Cyber hacking can also be used to retaliate, intimidate, or coerce others. For example, the IC has concluded that both North Korea and Iran view their ***cyber*** programs as vital to advancing political

---

[49] *See* Christopher Munsey, *Economic Espionage: Competing For Trade By Stealing Industrial Secrets*, FBI LAW ENFORCEMENT BULLETIN (Nov. 6, 2013), http://leb.fbi.gov/2013/octobernovember/economic-espionage-competing-for-trade-by-stealing-industrial-secrets.

[50] The Office of the National Counterintelligence Executive leads the government's counterintelligence efforts. The National Counterintelligence Executive is appointed by the Director of National ***Intelligence*** and currently also serves in a dual role as the Director of the National Counterintelligence and ***Security*** Center. NAT'L COUNTERINTELLIGENCE & ***SEC.*** CTR., http://ncsc.gov/about/director.html.

[51] *See* Randall C. Coleman, Assistant Dir., Counterintelligence Div., Fed. Bureau of Investigation, Statement Before the Senate Judiciary Committee on Crime and Terrorism (May 13, 2014), http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft; *see also* MCAFEE & CTR. FOR STRATEGIC AND INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND ***CYBER*** ESPIONAGE 4 (2013), http://www.mcafee.com/us/resources/reports/rpeconomic-impact-cybercrime.pdf.

[52] Kenneth L. Wainstein, Assistant Att'y Gen. for Nat'l ***Sec.***, U.S. Dep't of Justice, Press Conference Announcing Espionage Charges (Feb. 11, 2008), https://www.justice.gov/archive/nsd/2008/aag-nsd-080211.html (noting that foreign governments "want to steal our secrets and piggy-back on our technological innovation").

[53] *See* Fred Barbash & Abby Phillip, *Massive Data Hack of Health Insurer Anthem Potentially Exposes Millions*, WASH. POST (Feb. 5, 2015), http://www.washingtonpost.com/news/morningmix/wp/2015/02/05/massive-data-hack-of-health-insurer-anthem-exposes-millions/; Zachary Tracer,*Premera Blue Cross Says Data on 11 Million Exposed by Hackers*, BLOOMBERG (Mar. 17, 2015), http://www.bloomberg.com/news/articles/2015-03-17/premera-blue-cross-says-data-on-11-million-exposed-by-hackers; Nicole Perlroth,*Hack of Community Health Systems Affects 4.5 Million Patients*, N.Y. TIMES (Aug. 18, 2014), http://bits.blogs.nytimes.com/2014/08/18/hack-ofcommunity-health-systems-affects-4-5-million-patients/; Ellen Nakashima,*DHS Contractor Suffers Major Computer Breach, Officials Say*, WASH. POST (Aug. 6, 2014), https://www.washingtonpost.com/world/***national-security***/dhs-contractor-suffers-major-computerbreach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html.

objectives. [54] The most notorious such example to date may be the attack on Sony Pictures Entertainment. This attack destroyed Sony's computer systems, compromised private information, released valuable corporate data and intellectual property, and threatened employees, customers, and film distributers with violence. The attackers stole over 38 million files, totaling more than 100 terabytes of data. They released much of it to the public, attempting to tarnish the company's reputation and imposing significant financial and legal consequences. The data included private correspondence, unreleased films, salary records, and over 47,000 social ***security*** numbers. [55] The attack forced Sony to take its company-wide computer network offline and left thousands of its computers inoperable. [56] The hackers, originally styling themselves the "Guardians of Peace," threatened violence against theaters and filmgoers, referencing the 9/11 attacks. Their apparent motive was to retaliate against Sony for the planned Christmas Day release of *The Interview*, a comedy satirizing North Korean leader Kim Jong Un. Under immense pressure, Sony and **[*406]** leading movie theaters initially canceled the film's nationwide release (although it was later distributed). [57] Without firing a single shot, hackers derailed a major motion picture release that they found objectionable.

Political coercion through ***cyber*** means is not limited to state actors. Terrorist organizations also wield these tools to intimidate, disrupt, or degrade the performance of military and private sector systems. The conflict in Iraq and Syria is inspiring ***cyber*** attacks that have defaced websites and social media accounts used by the U.S. government. For example, on June 8, 2015, a hacker group called the Syrian Electronic Army (SEA) took credit for disabling an Army.mil website and defacing it with the statement: "Your commanders admit they are training the people they have sent you to die fighting." [58] The members of this group, too,

---

[54] ODNI WWTA 2015, *supra* note 36, at 3.

[55] *See* Keith Wagstaff, *Sony Hack Exposed 47,000 Social* ***Security*** *Numbers,* ***Security*** *Firm Says*, NBC NEWS (Dec. 5, 2014), http://www.nbcnews.com/storyline/sony-hack/sony-hack-exposed-47-000-social-***security***-numbers-***security***-firm-n262711.

[56] *See* Fed. Bureau of Investigation, *supra* note 46.

[57] *See "The Interview" to Screen in Select Theaters on Christmas*, CHI. TRIB. (Dec. 23, 2014), http://www.chicagotribune.com/entertainment/chi-interview-sony-release-20141223-story.html. The film had been scheduled to debut on over 3,000 screens across the country but ultimately opened in fewer than 300 independent theaters. Krishnadev Calamur,*"The Interview" Gets Nationwide Theatrical Release*, NAT'L PUB. RADIO (Dec. 25, 2014), http://www.npr.org/sections/thetwo-way/2014/12/25/373062179/the-interview-gets-nationwide-theatrical-release. To their great credit, both Google and Microsoft quickly agreed to distribute the movie through their online services.*See* Michael Cieply & Brooks Barnes, *Sony Streams "The Interview" on YouTube, Google Play and Xbox*, N.Y. TIMES (Dec. 24, 2014), http://www.nytimes.com/2014/12/25/business/sony-the-interview-online-streaming.html.

[58] Michael Hoffman, *Syrian Electronic Army Takes Down U.S. Army Website*, DEFENSE TECH (June 8, 2015), http://defensetech.org/2015/06/08/syrian-electronic-army-takes-down-us-armywebsite/. The SEA is a group of hackers who support Syrian President Bashar al-Assad.*See* Kate Vinton, *Syrian Electronic Army Claims Responsibility for Hacking U.S. Army Website*, FORBES (June 8, 2015), http://www.forbes.com/sites/katevinton/2015/06/08/syrian-electronic-army-claimsresponsibility-for-hacking-army-website/#4b467a46704d. U.S. Central Command (CENTCOM) suffered a similar attack in January 2015, when hackers purportedly affiliated with ISIL compromised CENTCOM's Twitter and YouTube accounts. As a result, its Twitter account read: "American Soldiers. We are coming. Watch your back. ISIS." Richard Sisk,*Central Command's Twitter, YouTube Hacked to Post Threats to Troops*, MILITARY.COM (Jan. 12, 2015), http://www.military.com/daily-news/2015/01/12/hackers-hit-centcom-sites-reveal-contact-infoand-issue-threats.html.

were recently charged for their conduct, [59] and one of the named defendants has already been successfully extradited to the United States to stand trial in federal court. [60]

Of note, many of these attacks are not driven by a single motivation. The SEA in particular has allegedly engaged in intrusions aimed not only at causing harm to the economic and ***national security*** interests of the United States, but also at lining SEA members' own pockets by extorting victims. We continue to see the threats and motivations blending. We see individual hackers supporting terrorist **[*407]** aims (Ferizi), groups defacing websites and simultaneously profiting from their criminal activities (SEA), and increasingly the lines between state actor, criminal group, and terrorist are blurring.

A final category of motivation is illustrated by network vulnerabilities that provide opportunities for our adversaries to engage in more strategic levels of harm. For example, consider a nation-state intent on changing the global landscape or disrupting the American way of life: connectivity provides it with ample opportunity to threaten our critical infrastructure. One example is our electric grid. Engineered in an analog age, the grid has been retooled for the digital age in a piecemeal fashion, creating major ***security*** flaws along the way. Modernization has been a double-edged sword: while it has unlocked new potential for efficiency and performance, it has also resulted in numerous connections to the Internet and new devices that increase the electric grid's susceptibility to ***cyber*** attack. Air-gaps--which once separated the grid and other vital systems like water treatment and industrial plants from the public Internet--are vanishing. [61] As a result, the industrial-control systems that manage and monitor many of our most important industrial facilities are exposed to hackers intent on wreaking havoc. [62] This is no longer merely a hypothetical concern. The Department of Homeland ***Security*** reported that a blackout in Ukraine in December 2015 that impacted more than 200,000 customers was caused by a ***cyber*** attack. [63]

While industrial-control systems are essential to cost-efficient and reliable power delivery, many of these systems were developed without a focus on ***security***. Encryption and authentication are often non-existent, [64] and automated, networked systems that allow a single supervisor to control multiple networks over a

---

[59] *See* Press Release, U.S. Dep't of Justice, Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army (Mar. 22, 2016), https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army..

[60] Press Release, U.S. Dep't of Justice, Syrian Electronic Army Member Extradited to the United States (May 10, 2016), https://www.justice.gov/usao-edva/pr/syrian-electronic-army-memberextradited-united-states.

[61] *See* RICHARD J. CAMPBELL, CONG. RESEARCH SERV., R43989: ***CYBERSECURITY*** ISSUES FOR THE BULK POWER SYSTEM 9 (2015) ("Over time, modification of SCADA [Supervisory Control and Data Acquisition] systems has resulted in connection of many of these older, legacy systems to the Internet."), https://www.fas.org/sgp/crs/misc/R43989.pdf.

[62] *See id.*

[63] *Alert (16-056-01): **Cyber**-Attack Against Ukrainian Critical Infrastructure*, ICS-CERT (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[64] *See* NAT'L INST. OF STANDARDS & TECH., GUIDE TO INDUS. CONTROL SYS. (ICS) ***SEC.*** 3-2, 3-14 (2011), http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (noting that "[m]any [ICS] systems may not have desired features including encryption capabilities" and that "[m]any ICS protocols have no authentication at any level").

wide geographic area create significant risk. [65] As Senator Sheldon Whitehouse warned in 2012, "[o]ur Nation will be vulnerable if critical infrastructure companies fail to meet basic ***security*** standards, as they do right now." [66]

[*408] These vulnerabilities have not gone unnoticed by our adversaries. As far back as November 2014, NSA Director Admiral Mike Rogers testified before Congress that his organization had already identified foreign intrusions into industrial-control systems in the United States, and that vulnerabilities in those systems were among his most pressing concerns. He described "reconnaissance by many . . . actors in an attempt to [e]nsure they understand our systems so that they can then, if they choose to, exploit the vulnerabilities within those control systems." [67] He went on to say that some state and non-state actors already possess the capability to access, impede, or shut down our basic infrastructure. [68] Just over a year later, we saw that statement proven true by the Bowman Dam intrusion. DNI Clapper likewise told Congress that "unspecified" Russian ***cyber*** actors are developing the skills to access those systems responsible for managing "critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks." [69]

* * *

Obviously, the government and the private sector need to (and will) [70] improve their defensive capabilities to anticipate these and future threats. But merely improving ***cybersecurity*** practices and building more resilient systems will not be enough. The difficult truth about ***cybersecurity*** is that the attacker always has the advantage. The defender must defend against all vulnerabilities at all times, whereas the attacker only has to succeed in one place at one time. [71] This difficulty is compounded by the incredible complexity of modern information technology systems.

When we first began confronting the full magnitude of the ***cyber*** threat, the focus was on defense and hardening our own systems. But defense is not enough. Because we lacked a more proactive strategy of deterrence and disruption, the rate of ***cyber*** intrusions and attacks continuously outpaced our ability to defend against them. [72]

---

[65] BIPARTISAN POLICY CTR., ***CYBERSECURITY*** AND THE NORTH AMERICAN ELECTRIC GRID: NEW POLICY APPROACHES TO ADDRESS AN EVOLVING THREAT 56-57 (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/***Cybersecurity***%20Electric%20Grid%20BPC.pdf.

[66] 158 CONG. REC. S4846-48 (daily ed. July 11, 2012) (statement of Sen. Sheldon Whitehouse).

[67] ***Cybersecurity*** *Threats: The Way Forward*: *Hearing Before the H. (Select)* ***Intelligence*** *Comm.*, 113th Cong. (2014) (statement of Adm. Michael Rogers, Commander of U.S. ***Cyber*** Command & Dir. of Nat'l ***Sec.*** Agency), https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml.

[68] *Id.*

[69] ODNI WWTA 2015, *supra* note 36, at 3; *see also Alert (14-281-01C): Ongoing Sophisticated Malware Campaign Compromising ICS (Update C)*, ICS-CERT (Dec. 10, 2014; last revised Jan. 26, 2016), https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[70] *See infra* Part III.C.

[71] *See* AT THE NEXUS OF ***CYBERSECURITY*** AND PUBLIC POLICY 36 (David Clark et al. eds., 2014).

[72] In particular, because ***cyber*** defenses are frequently insufficient, substantial effort has gone towards making networked systems more resilient to malicious activity.

Our strategy must be more proactive, and it must include deterrence. Our strategy must and will make clear that being shielded or sponsored by a foreign power will not offer protection. There can be no free passes. Homeland ***Security*** **[*409]** Advisor Lisa Monaco described our strategy for defending the United States from malicious ***cyber*** activity thus: "We will take steps . . . to protect our companies, to protect U.S. persons and to protect our interests in the time and place of our choosing." [73]

Of course, not all adversaries can be deterred. A nation-state stealing industrial secrets does so for economic reasons, and thus is sensitive to the costs--economic, diplomatic, and other--of getting caught. A terrorist group, on the other hand, may have pure destruction and intimidation as its aims, and won't care about the costs of getting caught. Thus, for some threats, disruption will remain the main strategy.

Part III lays out some of the ways the government can both deter and disrupt. Deterrence requires that we fundamentally change an attacker's costbenefit calculation by dramatically increasing the costs of bad behavior. Disruption requires that we stop the threat before an attack happens or achieves the desired effects. But to do either, we must first strip hackers of their real or perceived cloak of anonymity through public attribution, because if a hacker is invisible, his actions are cost-free. Attribution is the lynchpin of our success, and the topic to which this Article now turns.

II. Attribution and the Role of Investigations

There's no way around it: attributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act. Even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it. [74] Thus, technical investigation must often be supplemented by credible human ***intelligence***. [75] And all of this must be done quickly and consistently; attribution is of little use if it takes years and only identifies a small fraction of attackers.

Although attribution is difficult, it is far from impossible. Nor is the fundamental challenge new. For example, following 9/11, many were skeptical that the government could detect decentralized terrorist networks, let alone attribute specific attacks or conspiracies to individuals. Although the government tragically cannot stop every attack, since 9/11 the government has succeeded the **[*410]** vast majority of the time, in large part because of the contributions of ***national security*** investigators. And more generally, attributing bad acts is at the heart of law enforcement and ***intelligence*** gathering, both areas in which, along with the IC, DOJ plays a critical role.

This Part describes key components of our government's investigative toolkit, how they evolved to fight terrorism, and how the lessons from that evolution have shaped how we now confront the ***cyber*** threat.

A. *The Post-9/11* ***National Security*** *Evolution of the Department of Justice*

Before 2006, the ***national security*** activities of DOJ were divided among various and largely siloed components and offices. The attorneys prosecuting spies and terrorists and the attorneys who facilitated

---

[73] *Meet the Press Daily* (MSNBC television broadcast Sept. 29, 2015).

[74] *See* Taylor Armerding, *Whodunit? In Cybercrime, Attribution Is Not Easy*, CSO ONLINE (Feb. 5, 2015), http://www.csoonline.com/article/2881469/malware-cybercrime/whodunit-in-cybercrime-attribution-is-not-easy.html.

[75] *Id.*

intelligence collection against those same actors had little interaction. [76] This was by design; separating law enforcement and ***intelligence*** collection was thought to enhance the integrity of both, by preventing ***intelligence*** tools from improper use, preserving the independence of law enforcement, and protecting the sources and methods of ***intelligence*** collection. But this "wall" that separated foreign-***intelligence*** investigations from criminal ones worked to the detriment of both. [77] It hampered our efforts to bring terrorists and spies to justice, and impeded our ability to counter ***national security*** threats through comprehensive and effective ***intelligence*** collection.

The 9/11 Commission concluded that one factor hindering America's ability to prevent the deadly attacks of September 11, 2001 was this lack of coordination across the government, which led us to underestimate and respond slowly to threats. [78] The Commission specifically identified the wall that blocked information sharing between FBI investigators and DOJ prosecutors as a significant impediment to successful counterterrorism activities. [79] Two key **[*411]** developments--the passage of the USA PATRIOT Act [80] and a decision of the United States Foreign ***Intelligence*** Surveillance Court of Review [81]--dismantled this wall as a legal matter. [82]

But our work was not done. In 2005, with ***intelligence*** failure in Iraq making headlines, the Commission on the ***Intelligence*** Capabilities of the United States Regarding Weapons of Mass Destruction--established to explore deficiencies in U.S. ***intelligence*** gathering and analysis on weapons of mass destruction (WMDs) [83]--recommended the creation of a new AAG for ***National Security*** to oversee the ***national security***

---

[76] Historically, the primary ***national security*** entities of the Department were the Counterterrorism and Counterespionage Sections of the Criminal Division (CTS and CES respectively,) and the Counsel for ***Intelligence*** Policy in the Office of ***Intelligence*** Policy and Review (OIPR). *See* David Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L ***SEC.*** L. & POL'Y 1, 4 (2011) (describing the pre-9/11 "FISA wall" under which "law enforcement and ***intelligence*** were largely separate enterprises"); U.S. DEP'T OF JUSTICE, A.G. ORDER 2212-1999 (on file with author). The Executive Office for ***National Security***, established in 1994 within the Office of the Deputy Attorney General, provided basic coordination of ***national security*** activities within DOJ. Press Release, U.S. Dep't of Justice, New Executive Office for ***National Security*** Announced (Oct. 3, 1994), http://www.justice.gov/archive/opa/pr/Pre_96/October94/564.txt.html.

[77] *See* Kris, *supra* note 76, at 4-5; NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 78-79, 270-72 (2004) [hereinafter 9/11 COMMISSION REPORT].

[78] *See* 9/11 COMMISSION REPORT, *supra* note 77, at 348-49, 351-53.

[79] *Id.* at 79, 270-71. In 2004, Attorney General John Ashcroft attempted to bridge the divide by establishing the Justice ***Intelligence*** Coordination Council to coordinate ***intelligence*** practices across various agencies within the Department. *See* U.S. DEP'T OF JUSTICE, A.G. ORDER 2708-2004 (on file with author) (listing agencies involved).

[80] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

[81] In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

[82] *See generally* 1 DAVID S. KRIS & J. DOUGLAS WILSON, ***NATIONAL SECURITY*** INVESTIGATIONS AND PROSECUTIONS (2d ed. 2012).

[83] President Bush created the Commission by Executive Order. Exec. Order No. 13,328, 69 Fed. Reg. 6901 (Feb. 11, 2004).

activities of DOJ. [84] Acting on these recommendations, [85] in 2005, Congress passed the USA PATRIOT Reauthorization and Improvement Act and created the ***National Security*** Division (NSD) of DOJ. [86] It was the first new litigating division to be established in almost 50 years. [87] Its mission was and remains straightforward: to combat terrorism and other threats to ***national security***.

NSD's creation, along with other legislative and internal policy shifts, [88] helped eliminate organizational barriers that previously separated law enforcement from ***intelligence***, both legally and culturally, within DOJ. Functions that were once overseen by different leaders and pursued for different ends are now linked and coordinated. This facilitates greater collaboration and joint efforts among prosecutors, investigators, ***intelligence*** attorneys, and the IC. Integrating the efforts of ***intelligence*** and law enforcement personnel gives prosecutors and law enforcement agents access to ***intelligence***, allowing them to focus their resources and develop better criminal cases against the most significant targets. **[*412]** The record of NSD's success testifies to the power of this coordinated approach. We have disrupted countless terrorism plots and convicted hundreds of defendants in terrorism-related cases since the 9/11 attacks. [89] And we have collected a substantial amount of ***intelligence*** through these same investigations and prosecutions.

But notwithstanding the importance of the criminal justice system as part of our strategy, we also know that arrests and prosecutions are not always the best way to keep Americans safe. Counterterrorism prosecutors and agents recognize that the end goal is the disruption of the threat and protecting the safety of the public, regardless of the particular legal tool employed. That may mean sharing ***intelligence*** with a foreign partner to take action (including but not limited to local prosecution), preventing travel, freezing or seizing assets, warning the public, applying diplomatic pressure, imposing UN and domestic sanctions, supporting designations of groups as terrorist organizations, deploying ***intelligence*** operations, or executing military action. Criminal law and its enforcement may not always be central to, or even a component of, using those tools. And of course, our investigations often begin on the classified side. For this reason, in NSD, we have taken to referring to "investigations" generally, without regard to whether they are "criminal" or not. Of course, "***national security*** investigations" do typically involve criminal activity, and prosecution is a potential outcome that we work to preserve as often as we can--but it is a means to an end rather than our principal goal.

In recent years, we have taken a similar approach to addressing ***cyber*** threats--for example, through NSD's partnership with the Criminal Division. Computer crimes increasingly resist neat division into criminal and ***national security*** categories. Because the identity and goals of the hacker are often unknown at the outset

---

[84] COMM'N ON THE ***INTELLIGENCE*** CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, THE WMD COMMISSION REPORT 472-73 (2005), https://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf.

[85] *See* H.R. REP. NO. 109-333, § 506, at 109 (2005).

[86] USA PATRIOT Reauthorization and Improvement Act, Pub. L. No. 109-77, § 509A, 120 Stat. 192, 249 (2006).

[87] NAT'L ***SEC.*** DIV., U.S. DEP'T OF JUSTICE, PROGRESS REPORT (2008), http://www.justice.gov/sites/default/files/nsd/legacy/2014/07/23/nsd-progress-rpt-2008.pdf.

[88] *See* Kris, *supra* note 76, at 5 (citing USA PATRIOT Act); Memorandum from Att'y Gen. John Ashcroft to Various Dep't of Just. & FBI Officials, ***Intelligence*** Sharing Procedures for Foreign ***Intelligence*** and Foreign Counterintelligence Investigations Conducted by the FBI (Mar. 6, 2002), www.fas.org/irp/agency/doj/fisa/ag030602.html; In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

[89] Kris, *supra* note 76, at 14.

of a ***cyber*** intrusion, it is not always possible to segment investigations into clear criminal or ***national security*** categories. Many of the same technical, legal, and policy questions arise regardless of which Division handles a matter. And so, although both the Criminal Division and NSD conduct their own respective prosecutions (in partnership with U.S. Attorney's Offices), we increasingly find ourselves working cases jointly (or at least more actively supporting each other's cases). We also work together in the interagency policy process, where ***cybersecurity*** issues bear on both of our missions. As in our counterterrorism investigations, prosecution is one way to help protect our country from ***cyber*** threats, but it is not the only way.

Another example of collaboration among DOJ offices is the ***National Security Cyber*** Specialist (NSCS) network, a nationwide network of headquarters and field personnel trained and equipped to handle ***national security***-related ***cyber*** **[*413]** issues. [90] We established the NSCS network in 2012 to empower the field--to ensure that every jurisdiction has at least one specially trained ***national security*** prosecutor who not only is fluent with computers and networks, ***national security*** threats, and related investigative techniques and case law, but also is cleared to know the most sensitive threat information and is mindful of issues related to sensitive sources and methods that arise in ***national security*** investigations. It includes prosecutors from every U.S. Attorney's Office, along with experts from the Computer Crime and Intellectual Property Section of the Criminal Division and attorneys from all parts of NSD. It provides a simple means for two-way communication between the field and headquarters. This allows us to share information quickly and benefit from our respective areas of expertise in a breaking investigation. NSCS network attorneys receive specialized training on issues at the intersection of ***cyber*** and ***national security***, and the NSCS network leads outreach to private sector partners to raise awareness of the dangers posed by ***cyber*** threats and encourage closer relationships between the private sector and the government (before and after an intrusion).

Of course, the lawyers in DOJ could not do their jobs without the tireless work of the investigators and analysts of the FBI. At the heart of this effort is the FBI's ***Cyber*** Division, which has shifted since its inception in 2002 from targeting computer-enabled traditional crimes to addressing sophisticated ***cyber*** threats. The ***Cyber*** Division is a vital partner in our collective work and has evolved with the changing nature of the challenge.

One of the most significant threats we face is the increase in ***cyber*** espionage activity. Many of the most sophisticated threats we investigate are associated with nation-state actors or their proxies. In those matters, the FBI ***Cyber*** Division leads the investigation while coordinating closely with the FBI's Counterintelligence Division, which has historical expertise in the unique threats posed by nation-states. These divisions increasingly work together--for example, embedding Counterintelligence Division special agents and ***intelligence*** analysts within ***cyber*** operations and ***intelligence*** units. The Counterintelligence Division provided significant support to the ***Cyber*** Division during the economic espionage investigation that resulted in the indictment of five PLA actors in May 2014. [91]

In many ways, DOJ's increasingly close collaboration with the FBI on ***cyber*** matters is an example of how ***intelligence*** sharing within the U.S. government should operate. Soon after the NSCS network was formed, the FBI directed that new ***Cyber*** Task Forces--interagency teams based out of the FBI's **[*414]** 56 field

---

[90] *See generally* Press Release, U.S. Dep't of Justice, New Network Takes Aim at ***Cyber*** Threats to ***National Security*** (Nov. 14, 2012), http://www.justice.gov/opa/blog/new-network-takes-aimcyber-threats-***national-security***.

[91] Robert Anderson, Exec. Assistant Dir., Fed. Bureau of Investigation, Press Conference Announcing Charges Against Five Chinese Military Hackers (May 19, 2014), https://www.fbi.gov/news/speeches/combating-state-sponsored-***cyber***-espionage.

offices that are focused on ***cyber*** threats--engage in consistent communication with the NSCS representatives at the U.S. Attorney's Offices and share as much ***intelligence*** as possible, just as FBI and DOJ do in counterterrorism investigations. No longer are ***national security cyber*** threats deemed a matter solely for ***intelligence*** gathering and operations as opposed to investigations. Similar ***cyber intelligence*** sharing exists between DOJ and other agencies in the U.S. government, although we must continue to improve and deepen those ties.

Although we are applying the lessons we learned in the wake of 9/11 to our efforts to disrupt ***national security cyber*** threats, we have seen that there are new challenges that call for a new approach. After 9/11, the challenge was, as described above, tearing down the wall between law enforcement and ***intelligence***. In ***cybersecurity***, there is a third party involved--private entities. In ***cybersecurity***, this goes far beyond a generalized call to the public that "if you see something, say something." The private sector is now on the front lines, and often possesses the information we need to collectively respond to ***national security cyber*** threats. Information sharing is now a three-way affair, and successful collaboration on this front requires proactive outreach. This Article describes our outreach approach in more detail below. [92]

In sum, just as DOJ reorganized in the wake of 9/11 to more effectively counter the threat of international terrorism, DOJ is beginning to adapt to the threat that malicious ***cyber*** actors pose to ***national security***. And as the next section describes, one of the immediate benefits of this transformation has been the government's improved ability to attribute malicious ***cyber*** activity to the individuals, organizations, and nations responsible for it.

B. *Tools for Attribution*

We cannot effectively respond to a hack if we do not know who perpetrated it. Accordingly, the government must be able to gather and analyze information about ***cyber*** incidents quickly. "Online" investigations are in fact conducted mostly offline, which means that investigating a hack requires physically examining servers, talking to network users, and requesting or compelling providers to turn over copies of records. These are all classic techniques of law enforcement agencies. [93]

The Stored Communications Act [94] (SCA) is one of the government's most important authorities for gathering electronic evidence. The SCA sets out the **[*415]** procedures for federal and state law enforcement to obtain voluntary or compelled disclosure of stored communications from communications-service providers. [95] The SCA sets the procedural requirements based on the nature of the information

---

[92] *See infra* Part III.C.

[93] None of this is to downplay the important (and sensitive) tools that the IC, beyond just the FBI, brings to the effort to attribute, disrupt, and deter malicious ***cyber*** activity.

[94] 18 U.S.C. § 2701-2712. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). ECPA also amended the Wiretap Act and created the Pen Register and Trap and Trace Statute. Although practitioners often refer interchangeably to the SCA and ECPA, this Article refers to the SCA throughout.

[95] 18 U.S.C. § 2703. For an overview of the SCA, *see* COMPUT. CRIME & INTELLECTUAL PROP. ***SEC.***, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115-49 (3d ed. 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

sought. For instance, the government must obtain a search warrant to compel disclosure of content in many circumstances, while a subpoena is sufficient to compel disclosure of basic subscriber information. [96]

The Foreign ***Intelligence*** Surveillance Act of 1978 [97] (FISA) is a critical authority for ***national security*** or foreign ***intelligence*** investigations. [98] As a general matter, to obtain a FISA order for electronic surveillance conducted in the United States, the government must demonstrate, among other things, that the "target of the electronic surveillance is a foreign power or an agent of a foreign power;" [99] that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;" [100] and that "a significant purpose of the surveillance is to obtain foreign ***intelligence*** information." [101]

In addition, the government must frequently search and seize physical devices--for example, phones, computers, or servers--to effectively investigate and attribute malicious ***cyber*** activity. It can get the necessary authority to do so either through traditional search warrants [102] or, in the case of ***national security*** and foreign ***intelligence*** investigations, FISA orders. [103]

For the purposes of this Article, the intricacies of the legal authorities available to DOJ are less important than the following features they share in common. First, they are powerful tools that the government can use to investigate, and ultimately attribute, ***cyber*** intrusions and attacks. Second, they safeguard privacy by setting out a detailed and rigorous process by which the government must justify surveillance and manage the acquired information. And of course, the **[*416]** government is bound in all its activities to comply with the Constitution, including the Fourth Amendment.

In addition to its legal authorities, DOJ can draw on its institutional expertise to attribute hacks. The FBI has invested heavily in malware technical analysis capabilities. The FBI also hosts the National ***Cyber*** Investigative Joint Task Force, through which nineteen federal agencies coordinate ***cyber*** threat investigations. According to former ***National Security*** Agency General Counsel Stewart Baker, the view that hackers can operate with complete anonymity is antiquated: "[W]e *can* know who our attackers are . . . . The massive amount of data available online makes the job of attackers easier, but it can also help the defenders if we use it to find and punish our attackers." [104] These attribution efforts ensure that we have

---

[96] *Compare* 18 U.S.C. § 2703(a) (requiring search warrant to compel disclosure of "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less"), *with* 18 U.S.C. § 2703(c)(2) (permitting the use of a subpoena for basic subscriber and session information).

[97] Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[98] *See generally* 1 KRIS &WILSON, *supra* note 82.

[99] 50 U.S.C. § 1804(a)(3)(A).

[100] *Id.* § 1804(a)(3)(B).

[101] *Id.* § 1804(a)(6)(B).

[102] *See* FED. R. CRIM. P. 41.

[103] *See* 50 U.S.C. § 1822.

[104] *The Department of Homeland **Security** at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats: Hearing Before the S. Comm. on Homeland **Security** and Governmental Affairs*, 113th Cong. 1 (2013) (statement of Stewart A. Baker, Partner, Steptoe & Johnson LLP).

as complete a picture as possible of who ***cyber*** threat actors are and how particular actors conduct malicious ***cyber*** activity. For example, a key way the FBI attributed the Sony hack to North Korea was by comparing the malware used in that hack to malware used in other North Korea-sponsored ***cyber*** intrusions. [105]

Attribution requires tools beyond the technical analysis of malware. The FBI's National Center for the Analysis of Violent Crime contains several Behavioral Analysis Units that assist law enforcement with criminal investigative analysis for a wide range of offenses--from counterterrorism to bombings to white collar crime. [106] In 2012, the FBI created the ***Cyber*** Behavioral Analysis Center (CBAC), which expanded the work of the Behavior Analysis Units to ***cyber*** threats. By analyzing the behavioral patterns of malicious ***cyber*** actors--from the kind of malware they use, to the way they communicate with victims--the CBAC "profilers" use the traditional skills of law enforcement to help attribute malicious activity on the Internet.

The FBI used these traditional techniques, in addition to technical malware analysis, to attribute the Sony hacks to North Korea. In addition to the data-deletion malware, the Sony hackers left a "splash screen" on infected Sony computers with the name "Guardians of Peace" and various logos. The hackers used these images in ways similar to the behavior of criminals like serial killers who "stage" the crime scene, arranging it to send a message or conceal involvement. Such stagings go beyond what is necessary to commit the crime, and **[*417]** the extra information they disclose--as in the Sony case--can be helpful in attributing the activity.

More generally, prosecutors and agents are motivated and uniquely suited to investigate with the ultimate goal of using the uncovered information *publicly*. Working in law enforcement trains agents and prosecutors to pursue responsible individuals doggedly and to hold them accountable under the heavy burden of proof beyond a reasonable doubt in an open trial. That standard may be unattainable and unnecessary in the vast majority of cases where the government's response is something other than a criminal prosecution, but we benefit enormously from having a cadre of investigators that are trained to aim to meet a rigorous burden of proof with evidence that can be displayed publicly.

In addition to investigative expertise, prosecutors at DOJ and agents, investigators, and analysts at the FBI have a long history of working with private sector victims of criminal activity. Just as importantly, private sector entities are accustomed to working with the FBI and DOJ. This mutual trust and cooperation is critical, since the first step towards a successful attribution is to investigate the crime scene, which in the ***cyber*** context is frequently the victim's network--for example, a computer in the server room of a private company. Victims can provide valuable context, including why the bad actors wanted to do what they did when they did it.

This mix of authorities, institutional competence, and cooperative relationships has led to several high-profile public attributions of malicious ***cyber*** activity. In addition to the Sony case, for example, DOJ indicted five Chinese military officers for computer hacking, as described above. [107]

---

[105] *See* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks at the International Conference on ***Cyber Security***, Fordham University (Jan. 7, 2015), https://www.fbi.gov/news/speeches/addressing-the-***cyber***-***security***-threat.

[106] *See Investigative & Operations Support*, CRITICAL INCIDENT RESPONSE GRP., FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/cirg/investigations-and-operations-support.

[107] *See supra* notes 8-9 and accompanying text.

DOJ's decades of experience prosecuting espionage and export-control violations--violations that increasingly occur through ***cyber***-enabled means--have proven particularly valuable in facilitating attribution in ***cyber*** cases. For example, in August 2014, a federal grand jury indicted Su Bin, a 49-year-old Chinese businessman, on charges of unauthorized computer access, conspiracy to illegally export defense articles, and conspiracy to steal trade secrets. The indictment alleges that Su worked to "infiltrate computer systems and obtain confidential information about military programs, including the C-17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet." [108] Su pled guilty in March of this year. [109] In May 2015, six individuals, including three professors at Tianjin **[*418]** University in China, were charged with economic espionage, theft of trade secrets, and conspiracy. The indictment alleged that, over several years, the defendants "stole recipes, source code, specifications, presentations, design layouts and other documents marked as confidential and proprietary from the victim companies and shared the information with one another and with individuals working for Tianjin University." [110]

* * *

This Article began with a description of the ***cyber*** threat and why a good defense requires a strong offense--specifically, deterring bad actors from attempting their malicious activity. If actors believe they can attack in cyberspace anonymously, and at no cost to them, they have no incentive to stop. As deterrence is impossible without attribution, DOJ plays an important role in attributing malicious Internet activity to individuals, groups, and governments. The next Part catalogues the specific ways in which attribution enables DOJ, other federal agencies, and the private sector to take action.

III. An All-Tools Approach to ***National Security*** ***Cyber*** Threats

Sometimes the best response to malicious ***cyber*** activity will be a traditional criminal investigation or prosecution. Sometimes it won't. The right path is to adopt an "all-tools" posture by which decisions about how to respond are made in a threat-specific way, using, and if need be creating, the best and most appropriate tool or tools for the job, whatever they may be. And as this Part demonstrates, the most effective tools almost always require knowing whose fingers are at the keyboard on the other side of the screen.

A. *DOJ-Led Activity*

1. Prosecution

Federal prosecutors have at their disposal a wide array of statutes that address the full life cycle of a ***national security*** ***cyber*** threat--from inchoate planning to completed offenses. The most important such

---

[108] Press Release, U.S. Atty's Office, C.D. Cal., Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets (Aug. 15, 2014), https://www.fbi.gov/losangeles/press-releases/2014/los-angeles-grand-jury-indicts-chinese-national-in-computer-hacking-scheme-allegedly-involving-theft-of-trade-secrets; *see also* Indictment, United States v. Su Bin, No. 8:14-cr-00131-UA (C.D. Cal. Aug. 14, 2014).

[109] Press Release, U.S. Dep't of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information (Mar. 23, 2016), https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defensecontractors-systems-steal-sensitive.

[110] Press Release, U.S. Dep't of Justice, Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China (May 19, 2015), http://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-chargedeconomic-espionage-and-theft-trade-secrets; *see also* Superseding Indictment, United States v. Wei Pang, No. CR-15-00106-EJD (N.D. Cal. Apr. 1, 2015).

statute is the Computer Fraud and Abuse Act (CFAA), [111] a cornerstone statute that criminalizes computer crime generally, including most of what qualifies as ***national security*** computer crime. One common violation is "intentionally access[ing] a computer without **[*419]** authorization," thereby obtaining "information from any protected computer." [112] Another is intentionally accessing a protected computer without authorization and, as a result of such conduct, "caus[ing] damage and loss." [113] By way of example, the five PLA officers alleged to have stolen information for purposes of commercial advantage and private financial gain were charged with stealing information (a violation of 18 U.S.C. § 1030(a)(2)(C)), as well as the use of malware to control their victims' systems (a violation of § 1030(a)(5)). [114] Similarly, destructive malware used in the Saudi Aramco and Sony attacks and the typical DDoS attack would also violate § 1030(a)(5) (as would even less destructive website defacements commonly undertaken by terrorist or similar groups like the SEA).

Additional applicable statutes include the Wire Fraud statute, which criminalizes schemes to defraud "by means of false or fraudulent pretenses, representations, or promises . . . transmitted by means of wire," [115] and the Wiretap Act, which criminalizes the unlawful interception of wire communications, and the intentional disclosure and use of unlawfully intercepted communications. [116]

Prosecutors can also use statutes specifically focused on ***national security***. For example, the theft of trade secrets constitutes economic espionage under 18 U.S.C. § 1831 when the offense is committed with intent to benefit a foreign government, instrumentality, or agent--for example, a state-owned enterprise or the military of a foreign country. Section 1831 violations carry a higher statutory maximum than those under 18 U.S.C. § 1832, which prohibits trade-secrets theft generally. [117] This difference reflects the greater seriousness of a crime committed for a foreign power than for mere financial gain. In addition, the Arms Export Control Act [118] (AECA), the International Emergency Economic Powers Act [119] (IEEPA), and associated Executive Orders and regulations prohibit the export of controlled technology without a license, including through the theft of information and its transfer abroad over the Internet. The case against Su Bin was charged under the AECA and IEEPA.

Of course, it will be difficult to hale some charged individuals into a U.S. court, especially if they are located in--not to mention agents of--unfriendly **[*420]** ***foreign powers***. But history demonstrates that extradition works. The government will wait for as long as it may take to get custody over a defendant, as illustrated by our experience with international narcotics kingpins. For example, in 2012, Benjamin Arellano-Felix, the

---

[111] 18 U.S.C. § 1030.

[112] *Id.* § 1030(a)(2); *see also id.* § 1030(e)(2) (defining "protected computer").

[113] *Id.* § 1030(a)(5)(C).

[114] *See* PLA Indictment Summary, *supra* note 8.

[115] 18 U.S.C § 1343.

[116] *Id.* §§ 2510-2522.

[117] Individuals convicted under § 1832 may be fined or imprisoned up to 10 years, while individuals convicted under § 1831 may be fined up to $ 5 million or imprisoned up to 15 years. Organizations convicted under § 1832 may be fined up to $ 5 million, while organizations convicted under § 1831 may be fined the greater of $ 10 million or 3 times the value of what was stolen. 18 U.S.C. §§ 1831-1832.

[118] 22 U.S.C. § 2778.

[119] 50 U.S.C. §§ 1701-1708.

leader of the Tijuana Cartel, was convicted on federal racketeering and drug trafficking charges and, today, the 63-year-old drug lord is incarcerated in a U.S. prison. [120] He was originally indicted in 1997, at a time when extradition of a cartel leader was unprecedented. [121] He was arrested in 2002 and ultimately extradited for prosecution in 2011, proving that extradition can have tremendous success. And we are already seeing defendants in ***national security cyber*** cases being arrested on foreign soil and facing their charges in U.S. court, like the above-mentioned Su Bin and Ardit Ferizi.

But even if some fugitive hackers end up escaping justice before a federal judge, our general practice should nevertheless still be to publicly charge them as we do other defendants and with other crimes. First, publicly identifying perpetrators, as we did with the five PLA officers, reveals methods and signatures, thereby making it more difficult for them to continue hacking. This, along with worries about getting caught, can increase the cost--and thus decrease the frequency--of future intrusions against our systems. Second, indictments create consequences for the charged defendants themselves. Although our goal is to bring defendants before a court, naming them as wanted criminals also imposes costs. Hackers, like other thieves, are typically valued for their ability to get in and out of systems without getting caught. Their livelihood depends on anonymity. Hackers who are identified publicly by the authorities may find it more difficult to work. Potential "business" partners may be less likely to risk working with them (to avoid their own exposure), and employers may think twice before promoting them. They may be forced underground and face difficulty continuing their crimes, to the benefit of potential victims. Especially if public charges are combined with financial tools prohibiting transactions with indicted hackers, it will be more difficult for them to use the proceeds of their crimes. Finally, denying them the ability to travel, study, or work abroad (for fear of being arrested) imposes a high cost. To be forever cut off from most of the world is itself a restriction of liberty, especially for young hackers who are electronically well-connected to the outside world. These consequences deter not only the charged individuals, but others in their line of work.

Public charges also serve important expressive functions. Charging state-sponsored hackers signals that their behavior is a crime distinct from traditional espionage. [122] Imagine what would happen if we never stood up for the rights of **[*421]** U.S. companies whose secrets were stolen by foreign governments. Foreign actors would commit economic espionage with impunity. An understanding might develop that such behavior is, at least tacitly, acceptable. And if later we ever tried to challenge it, precedent would be against

---

[120] *See* Richard Marosi, *Former Drug Kingpin Arellano Felix Gets 25-Year Prison Term*, L.A. TIMES (Apr. 3, 2012), http://articles.latimes.com/2012/apr/03/local/la-me-arellano-felix-20120403.

[121] *See Under New Law, Mexico Extradites Suspect to U.S.*, N.Y. TIMES (May 5, 2001), http://www.nytimes.com/2001/05/05/world/under-new-law-mexico-extradites-suspect-to-us.html.

[122] Charging a criminal case also signals that the government has proof of its allegations and is prepared to back them up, publicly, and beyond a reasonable doubt. That was particularly important in 2014, when in the face of multiple public and private allegations of malicious activity by PRC officials, *see, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S ***CYBER*** ESPIONAGE UNITS (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; David E. Sanger et al.,*Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-againstus. html; Chris Strohm,*Chinese Hackers Seen Exploiting Cloud to Spy on U.S.*, BLOOMBERG (Nov. 20, 2013), http://www.bloomberg.com/news/articles/2013-11-20/chinese-hackers-seen-exploitingcloud-to-spy-on-u-s-. Chinese officials continued to deny their government engaged in any computer intrusions and challenged the United States to provide proof,*see, e.g., Beijing's Brand Ambassador: A Conversation with Cui Tiankai*, FOREIGN AFF. (July/Aug. 2013), https://www.foreignaffairs.com/interviews/2013-05-15/beijings-brand-ambassador) ("I don't think anybody has so far presented any hard evidence, evidence that could stand up in court, to prove that there is really somebody in China, Chinese nationals, that are doing these [cyberattacks].").

us. We would have granted our adversaries an easement of sorts--not over our territory, but over our intellectual and economic capital. Bringing public charges is akin to installing a giant "no trespass sign" on our front yard: Get off our lawn. International law is a law of custom, and our response in such a regime is critically important.

Thus, public charges can be particularly important where the United States seeks to persuade its allies of a norm of behavior. Charging PLA officers with hacking into U.S. entities to steal trade secrets for the economic benefit of Chinese companies clarified our position for the world. It likely helped lead Chinese President Xi to publicly agree to a proposed norm that China had been previously unwilling to accept. That norm provides that states should not "conduct or knowingly support ***cyber***-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." [123] This is a key development, since as Tom Donilon, former ***National Security*** Advisor to President Obama and the recently appointed head of the President's Commission on Enhancing ***Cybersecurity***, [124] said in a 2013 speech, "the United States and China, the world's two largest economies, both dependent on the Internet, must lead the way in addressing [the] problem" of ***cyber***-enabled economic espionage and trade-secrets theft. [125] This agreement, as noted above, was followed immediately by the G20's statement adopting norms of acceptable behavior in cyberspace.

[*422] Some commentators have expressed skepticism that the costs imposed by indictments of Chinese actors are sufficient to change Chinese behavior. [126] This argument against indictments oversimplifies the government strategy. Indictments of state-sponsored hackers will not prevent all malicious ***cyber*** activity. We need an all-tools, whole-of-government approach. The only way we can succeed is by changing how our adversaries analyze the costs and benefits of their actions. That is how we can help deter cyberattacks. And the effectiveness of this deterrence is dependent on attribution: knowing who our adversaries are and what makes them tick, whether at the level of country, government agency, organization, or individual hacker.

Again, this is no easy feat. That attribution may be difficult, however, is no reason to remove the criminal justice system from our toolkit. In fact, quite the opposite. DOJ and our law enforcement partners are uniquely well-suited to conduct these kinds of investigations. Through a mix of formal authority, ***cyber*** expertise, and cooperative relationships with private sector victims and international partners, we can track down ***cyber*** attackers and attribute their actions in a manner that can be used publicly. This public attribution is the bedrock of our approach because it facilitates the use of so many other tools--including sanctions, designations, and diplomatic options--that promote deterrence.

Further, we are at the very beginning of aggressively deterring state-sponsored ***cyber*** actors that engage in economic espionage and the theft of trade secrets. The goal is a world in which not only the United States

---

[123] White House, *supra* note 11.

[124] Press Release, O'Melveny & Myers LLP, Donilon to Lead White House Commission on National ***Cybersecurity*** (Feb. 18, 2016), https://www.omm.com/our-firm/media-center/pressreleases/donilon-to-lead-white-house-commission-on-national-***cybersecurity***/.

[125] Press Release, White House, Remarks by Tom Donilon, Nat'l ***Sec.*** Advisor to the President: "The United States and the Asia-Pacific in 2013" (Mar. 11, 2013), https://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-securityadvisor-president-united-states-an.

[126] *See, e.g.*, Jack Goldsmith, *China and Cybertheft: Did Action Follow Words?*, LAWFARE (Mar. 18, 2016), https://lawfareblog.com/china-and-cybertheft-did-action-follow-words.

but also other like-minded countries, aided by improved attribution techniques, use a variety of tools, including the criminal justice system, against malicious ***cyber*** actors as a matter of course. That is the relevant end state for analysis, and to those who are frustrated that we're not there yet, we agree; we should and must move faster. As to those who would abandon the use of indictments and prosecutions altogether, and prefer to do nothing, why give this conduct a free pass? As we have seen in the past, silence merely rewards bad behavior, and letting this behavior go on quietly unpunished is simply unacceptable.

We need to exert pressure on bad actors from every possible angle. Although prosecutions are just one tool in a broader approach [127] by which the U.S. can pressure actors like China, one should not underestimate the impact of public charges, especially with countries like China that are acutely sensitive to their international relationships. [128] Jim Lewis, Director and Senior Fellow at the **[*423]** Strategic Technologies Program at the Center for Strategic and International Studies, noted that "[t]he Chinese hated the indictments," and that the indictments played a "crucial role" in convincing China to change both its public and private stances on ***cyber***-enabled IP theft. [129]

The ultimate success of this approach will depend on the ability of U.S. agencies and departments to strengthen and support one another's actions. [130] That President Xi's commitments to the United States were followed by the adoption of this norm at the November 2015 G20 summit is very promising. Now, it is imperative that the U.S. take every possible action to see that these commitments come to fruition.

Finally, public charges can also have a positive effect on victims of ***cyber*** crimes. Charges recognize victims' injuries and reassure them that the U.S. government is dedicated to punishing the criminals who broke into their systems and stole their information. Victims want results, and charges let victims know that the perpetrators are not being given free passes. Public charges also strengthen public-private ***intelligence*** sharing relationships by providing concrete evidence to private entities that sharing information with the government gets results.

To be clear, legal culpability is always the key driver of the decision to prosecute. As explained in the United States Attorney's Manual, which provides internal guidance for DOJ attorneys prosecuting violations of federal law, the decision to bring charges requires that the prosecutor "believe[] that the person's conduct

---

[127] *See infra* Parts III.A.2 & 3.

[128] ***Cybersecurity*** *2015: China, China, China*, WASH. POST (Oct. 1, 2015), http://www.washingtonpost.com/video/postlive/***cybersecurity***-2015-china-china-china/2015/10/01/43919c26-6878-11e5-bdb6-6861f4521205_video.html. As former ***National Security*** Council Senior Director for Asian Affairs Evan Medeiros has explained, "[t]he big picture is that from 2014 on, the administration pursued a much more direct and coercive approach with China, and it has produced results over time." Ellen Nakashima,*Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/***national-security***/following-us-indictments-chinese-military-scaled-backhacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html. Former ***National Security*** Council Director for ***Cybersecurity*** Policy Robert Knake called the indictments a "strong move" and noted that the subsequent decrease in PLA ***cyber*** activity demonstrated that "China is not this implacable, immovable object" and that "[w]e can in fact alter the behavior of at least portions of the Chinese government."*Id; see also* Ellen Nakashima, *U.S. Developing Sanctions Against China over Cyberthefts*, WASH. POST (Aug. 30, 2015), https://www.washingtonpost.com/world/***national-security***/administration-developing-sanctionsagainst-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

[129] ***Cybersecurity*** *2015: China, China, China, supra* note 128, at 8:05 minutes.

[130] *See infra* Part III.B.

constitutes a Federal offense and that the admissible evidence will probably be sufficient to obtain and sustain a conviction." [131] Thus, although the non-prosecutorial benefits described above are important, they must always be secondary considerations in any charging decision.

[*424] Criminal prosecutions are an effective legal action that can be taken after we have attributed a hack, but they are far from the only one. In those situations where we have not brought formal charges, we may still gain some of the benefits described above--norm-building, damage to hackers' reputations, etc.--merely through public attribution itself. This gives the government great flexibility as to when to bring public charges, knowing that, even in those situations in which charges are not brought, public attribution can have profound deterrent and disruptive effects on our ***cyber*** adversaries.

2. Other Civil and Criminal Actions

In addition to indictments and prosecutions, the U.S. government can use other civil and criminal authorities--including injunctions and temporary restraining orders against fraud and illegal interception of communications, as well as seizure warrants--to fight hackers. Although most of the examples I cite below involve activity designed to advance traditional criminal objectives, they show what's possible in the ***national security*** context, given the increasing convergence in the ***cyber*** tools used by sophisticated criminal, terrorist, and nation-state actors.

In 2011, the Justice Department's Criminal Division, the U.S. Attorney's Office for the District of Connecticut, and the FBI disrupted the Coreflood botnet--which had seized control of over 2.3 million infected computers, including 1.8 million in the United States--using a combination of civil injunctive authorities and criminal search warrants. [132] The Coreflood malware was a virus that allowed criminal operators to steal online banking credentials and other information from unsuspecting users by tracking their every keystroke. [133] The program forced infected computers to repeatedly check in with command-and-control servers, and then receive and execute commands. The criminals behind this scheme used Coreflood to steal hundreds of thousands of dollars through fraudulent wire transfers from victims, most of whom were small- or medium-sized businesses and local governments. [134] **[*425]** The government obtained seizure warrants to take down the commandand-control servers and confiscate the domain names used to transmit communications between those servers and infected computers. [135] After seizing the illegal hardware, the government

---

[131] U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-27.220, https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.220.

[132] Copies of the related court documents are available at Press Release, U.S. Dep't of Justice, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm. For additional coverage, see also Jason Ryan,*Feds Take "Coreflood Botnet": "Zombie" Army May Have Infected 2 Million Computers, Stolen Hundreds of Millions of Dollars*, ABC NEWS (Apr. 13, 2011), http://abcnews.go.com/technology/feds-crush-coreflood-botnet-infected-million-computers-stole/story?id=13369529.

[133] Coreflood is an example of what is referred to as a "keylogger": a program that records and transmits what users enter through their keyboards.

[134] *See Botnet Operation Disabled: FBI Seizes Servers to Stop* ***Cyber*** *Fraud*, FED. BUREAU OF INVESTIGATION (Apr. 14, 2011), https://www.fbi.gov/news/stories/2011/april/botnet_041411; David B. Fein,*Major Achievements in the Courtroom: Coreflood Botnet Takedown & Civil Action*, U.S. DEP'T OF JUSTICE (July 9, 2015) http://www.justice.gov/usao/priority-areas/cybercrime/major-achievements-courtroom-coreflood-botnet-takedown-civil-action.

[135] *See* Seizure Warrant, In re Seizure of the Premises Known and Described as Twenty-Four Certain Internet Domain Names (Apr. 12, 2011), https://www.fbi.gov/newhaven/pressreleases/2011/pdf/nh041311_2.pdf.

obtained a federal injunction as authorized by fraud [136] and wiretapping [137] statutes. The injunction gave the government the authority to redirect infected computers to secure substitute servers that could command the virus to stop running on infected computers. [138] More importantly, the injunctive remedies prevented Coreflood from updating itself. [139] Antivirus companies, in partnership with the government, then developed updated virus signatures that could detect and delete Coreflood from innocent computers. The FBI also worked closely with Internet service providers (ISPs) to identify and notify individuals whose computers had been infected. As of today, using these law enforcement authorities, we have successfully erased Coreflood from 95% of infected computers. [140]

This unprecedented law enforcement operation employed a combination of criminal and civil authorities against an international hacking ring. Notably, these authorities predate the modern Internet, and in some cases, predate computers. For example, the concept of an injunction to prevent ongoing illegal activity dates back to pre-Revolutionary law, and the specific statutes invoked for injunctive authority date to the 1980s. But all of these authorities were used in 2011 to take down a very modern ***cyber*** threat.

More recently, the FBI neutralized the GameOver Zeus botnet, which was responsible for an estimated $ 100 million in losses from businesses and consumers worldwide whose banking credentials were compromised. [141] One senior FBI official described this "peer-to-peer" network as the most sophisticated botnet the FBI had ever attempted to disrupt. [142] To bring down this criminal network, the U.S. Attorney's Office for the Western District of Pennsylvania, **[*426]** along with DOJ's Criminal Division and the FBI, obtained injunctive relief authorizing them to sever communications between infected botnet computers and the criminal command-and-control servers. [143] That intercession allowed law enforcement to redirect innocent computers to substitute servers under government control. In other words, the government stepped in between the hackers and the victims, and redirected the victims toward a safer place. As of July 2014, all or nearly all of the computers infected with the GameOver Zeus virus had been "liberated from

---

[136] *See* 18 U.S.C. § 1345.

[137] *See id*. § 2521.

[138] For copies of the related court documents, see Press Release, Fed. Bureau of Investigation, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm.

[139] *See* Seizure Warrant, *supra* note 135.

[140] Fein, *supra* note 134.

[141] *See* Press Release, Fed. Bureau of Investigation, GameOver Zeus Botnet Disrupted: Collaborative Effort Among International Partners (June 2, 2014), https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted; Tony Bradley,*How to Protect Yourself Against Gameover Zeus and Other Botnets*, PCWORLD (June 2, 2014), http://www.pcwor ld.com/article/2357528/protect-yourself-against-gameover-zeus-and-other-botnets.html.

[142] Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-andcryptolocker-ransomware.

[143] *See* Memorandum of Law in Support of Motion for TRO and Order to Show Cause at 20, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. June 2, 2014), https://www.justice.gov/opa/file/783651/download.

the criminals' control." [144] The same authorities that facilitated this intervention in the criminal context could be used to address ***national security*** ***cyber*** threats.

At the same time that law enforcement agencies were pursuing civil orders to mitigate the botnet's substantial damage, a parallel and complementary law enforcement investigation was also working to identify and prosecute the particular individuals behind this global scheme. One of those individuals, Evgeniy Bogachev, now ranks as one of the FBI's most wanted criminals. In May 2014, a grand jury in Pittsburgh unsealed an indictment identifying Bogachev as the mastermind behind GameOver Zeus and charging him with over a dozen crimes, including conspiracy, computer hacking, bank fraud, wire fraud, and money laundering. [145]

The same operation that brought down GameOver Zeus was used to target the malware CryptoLocker, which the botnet had implanted on hundreds of thousands of computers around the world. As described above, CryptoLocker is a "ransomware" program that infects computers, encrypts files, and demands a ransom of hundreds of dollars in order to decrypt the files. [146] The GameOver Zeus botnet contains features that allow users to install additional malware on infected computers, and CryptoLocker was one of the most popular choices. At the time the United States sought to bring it down, CryptoLocker had already infected more than 230,000 computers, including more than 120,000 in the United States. [147] One report estimated that victims of this scheme paid $ 27 million in ransom payments in the final months of 2013. [148]

[*427] The FBI and DOJ used similarly innovative legal tools to take apart the botnet used in the Iranian DDoS attack against the U.S. financial sector. Through its FBI Liaison Alert System (more commonly known as FLASH), the FBI regularly updated the private sector with information on the botnet. The FBI has also directly contacted ISPs that host victim computers, providing information and assistance on removing the malware. This has led to a near-complete dismantling of the botnet. [149]

3. New Proposals

As the above suggests, law enforcement authorities have more at their disposal than criminal charges. Our tools include search warrants, subpoenas, injunctions, temporary restraining orders, asset forfeiture, and voluntary private sector cooperation--all of which can have operational benefits. A variety of investigative activities also help us understand the threat and how we can assist private citizens to guard against it.

---

[144] Press Release, U.S. Dep't of Justice, Department of Justice Provides Update on GameOver Zeus and Cryptolocker Disruption (July 11, 2014), https://www.justice.gov/opa/pr/us-leads-multinational-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[145] *See* Indictment at 11-22, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. May 19, 2014), http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf.

[146] *See supra* note 26 and accompanying text.

[147] *Id*. at 9.

[148] Violet Blue, *CryptoLocker's Crimewave: A Trail of Millions in Laundered Bitcoin*, ZDNET (Dec. 22, 2013) http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-inlaundered-bitcoin/.

[149] Press Release, U.S. Dep't of Justice, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of ***Cyber*** Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iraniansworking-islamic-revolutionary-guard-corps-affiliated-entities-charged.

Yet these legal authorities are not enough. We must update our laws to confront the modern threat. The Obama Administration has made a number of proposals to refine and expand the government's authority to conduct these types of operations. The statutes used in the Coreflood and GameOver Zeus operations give federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping. [150] Because the criminals behind Coreflood and GameOver Zeus used them to commit fraud against banks and bank customers, existing laws allowed DOJ to obtain court orders to disrupt the botnets. But the authority to shut down botnets that are not engaged in fraud or wiretapping is unclear. [151] That is why, as part of a larger legislative package, the President proposed to Congress in January 2015 that activities like the operation of a botnet be added to the list of offenses eligible for injunctive relief. Specifically, the amendment would permit the department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. [152]

DOJ also submitted a proposal to amend Rule 41 of the Federal Rules of Criminal Procedure to modernize those provisions governing the territorial **[*428]** boundaries for searches of stored electronic media. Under the current Rule 41(b), magistrate judges are empowered to issue search warrants for physical items within the confines of their districts, with a few limited exceptions for out-of-district warrants. While this framework historically facilitated law enforcement investigations, the proliferation of network-based criminal activity is evading these once-rational restrictions. As the then-Acting AAG for the Criminal Division explained, the current rule does not "directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks." [153] Specifically, it makes no provision for situations where the computer to be searched via remote access cannot be physically located or where numerous computers spread across multiple districts must be searched or seized at once, as in a botnet takedown. A revision to the rules recommended by DOJ would close these loopholes and arm investigators with the tools they need to address a range of criminal conduct that is currently evading our efforts. The Supreme Court transmitted the revision to Congress in April 2016. [154]

B. *DOJ's Role in a Whole-of-Government Approach*

DOJ's investigations also enable a variety of responses that make use of the legal authorities of other departments and agencies. In particular, by attributing malicious ***cyber*** activity to its source, lawyers and investigators enable smart, targeted action to punish ***cyber*** criminals and deter future would-be bad actors.

For example, attribution will play a critical role in using economic sanctions to counter malicious ***cyber*** activity. On April 1, 2015, the President issued an Executive Order (EO) that will allow the use of America's economic power against the foreign ***cyber*** threat. EO 13,694, entitled "Blocking the Property of Certain Persons Engaging in Significant Malicious ***Cyber***-Enabled Activities," authorizes the Treasury Secretary, in consultation with the Attorney General and the Secretary of State, to impose targeted sanctions on and

---

[150] 18 U.S.C. §§ 1345, 2521.

[151] *See* Leslie R. Caldwell, *Assuring Authority for Courts to Shut Down Botnets*, U.S. DEP'T OF JUSTICE (Mar. 11, 2015), http://www.justice.gov/opa/blog/assuring-authority-courts-shut-downbotnets.

[152] *See* WHITE HOUSE, UPDATED ADMINISTRATION PROPOSAL: LAW ENFORCEMENT PROVISIONS, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcementtools-section-by-section.pdf.

[153] Letter from Mythili Raman, Acting Assistant Att'y Gen., Crim. Div., U.S. Dep't of Justice (Sept. 18, 2013) (on file with author).

[154] *Pending Rules Amendments*, U.S. COURTS, http://www.uscourts.gov/rules-policies/pendingrules-amendments.

block the assets of individuals and entities whose "malicious ***cyber***-enabled activities" originating from outside the United States contribute to a significant threat to the ***national security***, foreign policy, economic health, or financial stability of the United States. [155]

[*429] Among other things, this EO allows the U.S. government to target certain companies that benefit from trade-secrets theft. Specifically, if a foreign individual or entity receives or uses a trade secret misappropriated through cyberenabled means, knows the trade secret was misappropriated, and meets certain other criteria, then they could be subject to sanctions under the EO. Economic sanctions carry severe consequences: access to company property in the United States is blocked and U.S. individuals and firms are generally prohibited from engaging in transactions or dealing with that company. This EO has the potential to successfully deter foreign companies and individuals outside our jurisdiction. The types of narrowly tailored sanctions authorized by the EO have the potential to "make clear that the United States and its partners are willing to take a more forceful stance to uphold norms of good conduct in cyberspace," without eliciting the damaging impact on the U.S. and world economies that broad-based sanctions might. [156] Although the EO has not yet been used, it will no doubt change the calculation of foreign parties, including those who are contemplating whether to accept or use American trade secrets stolen by their governments. Similarly, sharing information with partners in the State Department and the U.S. Trade Representative's Office allow those partners to use the tools available to them more effectively.

Imposing economic sanctions on an entity often requires tracing the misappropriated trade secrets to their source--in other words, attributing the ***cyber*** intrusion and theft. In addition, knowing who stole the data can be helpful in tracing the spread of that data to companies that use it despite knowing that it's stolen. Accordingly, DOJ investigations will undoubtedly contribute substantially to the development of sanctions targets under this EO, as they often do under other legal tools. Such tools include the Commerce Department-administered Entity List, by which individuals or organizations can be barred from receiving U.S. exports if their activities are contrary to U.S. ***national security*** or foreign policy interests. [157] For example, the Commerce Department placed both Su Bin and his aviation company on the Entity List around the time of his indictment. [158] In addition, there are EOs that block property of, and prohibit transactions with, individuals who commit or support terrorism or the proliferation of WMDs. [159]

Finally, effective diplomatic and military responses to malicious ***cyber*** activity also require knowing who committed the bad acts. For example, the public criticism of North Korea for the Sony hacks, as well as the additional **[*430]** economic sanctions imposed in early 2015, [160] could not have occurred without the FBI's activities, in partnership with Sony, to uncover who was responsible for the intrusion into Sony's

---

[155] Press Release, White House, Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious ***Cyber***-Enabled Activities" (Apr. 2, 2015), https://www.whitehouse.gov/the-press-office/2015/04/02/statement-president-executiveorder-blocking-property-certain-persons-en.

[156] Zack Cooper & Eric Lorber, *Sanctioning the Dragon: Using Statecraft to Shape Chinese Behavior*, LAWFARE (Mar. 13, 2016), https://www.lawfareblog.com/sanctioning-dragon-usingstatecraft-shape-chinese-behavior.

[157] *See Entity List*, BUREAU OF INDUS. & ***SEC.***, U.S. DEP'T OF COMMERCE, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

[158] *See* 78 Fed. Reg. 44,680, 44,681 (Aug. 1, 2014); *see also* 81 Fed. Reg. 14,953, 14,957 (Mar. 21, 2016).

[159] *See* Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001) (terrorism); Exec. Order No. 13,382, 70 Fed. Reg. 38,567 (July 1, 2005) (WMD).

[160] Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015).

systems. Nor could an important collateral benefit of the PLA indictment--the pressure it put on China to agree to change its behavior with respect to economic espionage--have occurred had DOJ been unable to identify the Pittsburgh hackers as PLA officers. Diplomatic efforts have proven critical in China's acceptance of international ***security*** norms in the past--notably in the field of export control and nonproliferation, where, as former ***National Security*** Council Director for Asian Affairs Evan Medeiros has noted, U.S. pressure "played an important role." [161] DOJ contributed to that effort by, in the words of former AAG for ***National Security*** J. Patrick Rowan, "taking many of the concepts used in combatting terrorism--namely, prevention, cooperation and coordination--and applying them to the efforts to prevent the illegal export of sensitive U.S. technology." [162] In a similar way, we will be able to use our ability to attribute malicious ***cyber*** activity to push other countries toward accepting and abiding by ***cyber*** norms. Finally, if the U.S. government ever needs to respond to a major ***cyber*** attack with military or ***intelligence*** operations, [163] accurate and rapid attribution will be critical.

C. *Public-Private Collaboration*

The private sector and government have long worked together to strengthen the national defense. During the Cold War, this generally involved volunteers and civil defense functions largely divorced from actual conflict--the battlefields were never on U.S. soil. [164] Today, some of the greatest dangers to ***national security*** transit electronic networks reside *within* our borders, threatening, among other things, critical infrastructure that supports our domestic economy **[*431]** and our health and safety. Private actors, not the government, are the dominant players, and the role of the private sector will only continue to increase as the "Internet of Things" gains increasing importance in our daily lives. [165] ***Cybersecurity*** must be built into all phases of development of Internet-connected systems and devices. This need was made evident when, just last July, ***security*** researchers remotely hacked a Jeep Cherokee as it was being driven down

---

[161] EVAN S. MEDEIROS, RAND CORP., CHASING THE DRAGON: ASSESSING CHINA'S SYSTEM OF EXPORT CONTROLS FOR WMD-RELATED GOODS AND TECHNOLOGIES 17 (2005), http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG353.pdf; *see also* EVAN S. MEDEIROS, RAND CORP., CHINA'S INTERNATIONAL BEHAVIOR: ACTIVISM, OPPORTUNISM, AND DIVERSIFICATION 98 (2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG850.pdf ("Chinese policymakers and analysts regularly stress the high quality of U.S.-China cooperation on combating global terrorism and WMD proliferation, highlighting it as a new basis of stability in bilateral relations.").

[162] *Enforcement of Federal Espionage Laws: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland* ***Security*** *of the H. Comm. on the Judiciary*, 110th Cong. 5 (2008) (statement of J. Patrick Rowan, Dep. Assistant Att'y Gen., Nat'l ***Sec.*** Div., U.S. Dep't of Just.).

[163] *See, e.g.*, DEP'T OF DEF., THE DOD ***CYBER*** STRATEGY 11 (2015), http://www.defense.gov/Portals/1/features/2015/0415_***cyber***-strategy/Final_2015_DoD_***CYBER***_STRATEGY_for_web.pdf ("The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. . . . The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.").

[164] NAT'L PREPAREDNESS TASK FORCE, U.S. DEP'T OF HOMELAND ***SEC.***, CIVIL DEFENSE AND HOMELAND ***SECURITY***: A SHORT HISTORY OF NATIONAL PREPAREDNESS EFFORTS 5-7 (2006), http://training.fema.gov/hiedu/docs/dhs%20civil%20defense-hs%20-%20short%20history.pdf.

[165] For an analysis of coming ***cybersecurity*** risks, see SOFTWARE ENG'G INST., CARNEGIE MELLON UNIV., 2016 EMERGING TECHNOLOGY DOMAINS RISK SURVEY (2016), http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf.

a highway, gaining the ability to shut down the engine, disable the brakes, and affect steering. [166] As a result of that controlled experiment, Chrysler issued a recall for 1.4 million vehicles. [167] It will be far cheaper, and far more beneficial to our collective ***security***, if companies invest in ***cybersecurity*** at the front end of the product design and development process.

Not only is the majority of Internet-connected devices and Internet software and traffic privately used and generated, but the Internet's physical networks are also managed by private corporations. Over 80% of the critical infrastructure in the United States is owned and controlled by private firms. [168] Despite the tremendous resources and expertise available to federal agencies, the private sector is an indispensable partner in securing our nation's digital systems. [169] As my predecessor Lisa Monaco explained: "Private companies are on the front lines. Individual defenses, as well as broader efforts to reform . . . will require our joint efforts." [170] ISPs, critical-infrastructure operators, software vendors, ***security*** researchers, and industry associations all have important roles to play. Our collective success in protecting the country from the economic and physical consequences of network intrusions will depend in large part on the effectiveness of public-private collaborations.

As in the days after 9/11, when we tore down the wall between law enforcement and ***intelligence***, now we facilitate information and threat sharing between the government and the private sector. Without cooperation and information from the private sector, the government would have a much harder **[*432]** time attributing malicious ***cyber*** activity and understanding its motivations. At the same time, the private sector relies on the government for information about the latest threats and to take investigative and deterrent actions unavailable to the private sector. Senator Dianne Feinstein has emphasized the importance of publicprivate cooperation in ***cybersecurity***: "To strengthen our networks, the government and private sector need to share information about the attacks they are facing and how best to defend against them." [171]

Companies sometimes hesitate to voluntarily share information with the government. This is understandable. They may worry that sharing information about ***cyber*** intrusions with law enforcement or regulators might risk their public reputation, customer confidence, or stock prices, and that doing so could

---

[166] Michael E. Miller, *"Car Hacking" Just Got Real: In Experiment, Hackers Disable SUV on Busy Highway*, WASH. POST (July 22, 2015), https://www.washingtonpost.com/news/morningmix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/.

[167] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, WIRED (July 24, 2015), http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[168] U.S. GOV'T ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTORS' CHARACTERISTICS (2006) http://www.gao.gov/assets/260/252603.pdf.

[169] *See Critical Infrastructure Sector Partnerships*, U.S. DEP'T OF HOMELAND ***SEC.***, http://www.dhs.gov/critical-infrastructure-sector-partnerships; Myriam Dunn Cavelty & Manuel Suter,*Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection*, 4 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION 179 (2009).

[170] Lisa Monaco, Assistant Att'y Gen. for Nat'l ***Sec.***, U.S. Dep't of Justice, Speech at the 2012 Cybercrime Conference, Seattle (Oct. 25, 2012), http://www.justice.gov/nsd/justice-news-2.

[171] Press Release, U.S. Senate Select Comm. on ***Intelligence***, Senate ***Intelligence*** Committee Approves ***Cybersecurity*** Bill (July 10, 2014), http://www.***intelligence***.senate.gov/press/senateintelligence-committee-approves-***cybersecurity***-bill.

expose them to litigation, enforcement actions, or even criminal sanctions. Even where regulatory guidance requires disclosure, "companies have tended to include generic risk factors rather than disclose specific incidents," according to former Acting AAG Todd Hinnen. [172] With business concerns in mind, companies may prefer to conduct an investigation internally in an attempt to resolve the problem on their own before involving law enforcement. If they do resolve it, the incident may never be reported; if they do not, the reporting and subsequent investigation will be delayed.

There are risks to going it alone, both for the individual victim company and the public at large, and reasons why reporting intrusions to law enforcement is to a company's advantage. First and foremost, the government can help victims understand what happened. Experienced law enforcement agents (with access to the ***intelligence*** and resources of other parts of the government) are often familiar with patterns of malicious ***cyber*** activity across the country. They can help a company's ***security*** and technical teams identify and stop the malicious activity and better understand the context of the incident.

As a result, private reporting can help reveal what may have initially appeared to be a simple criminal enterprise as something much more sinister. Consider the complaint in the Ferizi case, mentioned above. [173] To the victim company, the intrusion into its network and the theft of personally identifiable information may have appeared to be simple identity theft of a sort perpetrated every day in this country. But the government was in the position to uncover that, as alleged in the complaint, the ***cyber*** activity was part of a transnational terrorist threat, involving a Kosovar citizen in Malaysia providing personally identifiable information on American service members to ISIL. But imagine **[*433]** (counterfactually) if the victim decided not to cooperate with law enforcement to investigate the origin and scope of the intrusion, and physical harm befell one of the individuals whose data was stolen. The repercussions to the victim company might go beyond the data breach alone.

Furthermore, if one company discovers a ***cyber*** intrusion, it is likely that other companies in the industry have been breached as well. Usually, perpetrators of ***cyber*** intrusions use exploits that target common vulnerabilities, and many perpetrators engage in mass exploitation of targets. Reporting the incident allows law enforcement to identify broader trends in the ***cyber*** threat environment and to disseminate information that helps other potential victims protect their own networks. And disclosing information about the intrusion to the U.S. government often enables us to share valuable insights and information from other investigations with the reporting victim. The more complete a victim's understanding of what happened, the better its ability to mitigate any damage and to identify and defend against similar activity in the future.

Second, proactive cooperation may assist victims in dealing with government regulators and other constituents. For instance, the Federal Trade Commission has said that it's "likely" that it will view a company that has suffered a breach "more favorably" if "it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion." [174] And the

---

[172] *See* Karen Freifeld, *U.S. Companies Allowed to Delay Disclosure of Data Breaches*, REUTERS (Jan. 16, 2014), http://www.reuters.com/article/us-target-data-notification-idUSBREA0F1LO20140116.

[173] *See supra* notes 38-39 and accompanying text.

[174] Mark Eichorn, *If the FTC Comes to Call*, FED. TRADE COMM'N BUS. BLOG (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call ("We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the

Securities and Exchange Commission has signaled that it "will give substantial credit" to companies that proactively self-report ***cyber*** intrusions. [175] Cooperation also often strengthens a victim's position before shareholders, insurers, lawmakers, the media, and others observing how it responds. As our outreach has shown, those constituents want to know whether the company did everything in its power to protect itself (and often its customers), and that includes cooperating with law enforcement.

Third, the federal government is uniquely positioned to win some measure of justice for victims and to deter malicious activity. This may, of course, be through criminal charges, arrest, and prosecution. But when victims report intrusions and cooperate in ensuing investigations, they also enable every one of the other legal tools and actions discussed in the foregoing sections. These include diplomatic pressure, ***intelligence*** operations, military action, enforcement of **[*434]** multilateral trade agreements, and economic sanctions. These tools not only deter foreign actors generally, but also can potentially target the individual companies that benefit from the economic espionage, thus providing a measure of specific deterrence and possibly mitigation of damage.

Because electronic evidence dissipates over time, speed is essential in breach investigations. We can't know today whether we will charge a case, arrest a defendant, or take some other action, but quick action to report and investigate a breach maximizes the chances that we are able to take some legal or other action to disrupt the perpetrators.

On the other hand, without private reporting of ***cyber*** incidents and indicators, there is little deterrence: hackers can easily find new targets and run little risk of punishment. Fortunately, last December, and after close to eight years of congressional consideration of legislation to address this problem, the President signed legislation to encourage public-private collaboration related to the sharing of certain types of ***cyber*** information. The ***Cybersecurity*** Information Sharing Act of 2015 provides companies with certain liability protection when they share indicators of ***cyber*** threats, or techniques to defend against ***cyber*** threats, with each other and with the government. [176] The legislation also includes rigorous requirements and restrictions to ensure that privacy and civil liberties are protected, including through requirements to remove personal or identifying information [177] and guidelines to "limit the receipt, retention, use, and dissemination of ***cyber*** threat indicators containing personal information or information that identifies specific persons." [178]

Finally, sometimes the government alone has access to the critical ***cyber*** threat signatures that private industry needs to effectively defend itself. In addition to the Department of Homeland ***Security***, which runs the important Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems

---

breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.").

[175] Ken Herzinger et al., *SEC Speaks--What to Expect in 2016*, ORRICK (Feb. 23, 2016), http://blogs.orrick.com/***securities***-litigation/2016/02/23/sec-speaks-what-to-expect-in-2016/.

[176] Consolidated Appropriations Act, 2016, Pub. L. 114-113, div. N, tit. I, 129 Stat. 2241, 2936 (2015) (codified at 6 U.S.C. §§ 1501-1510).

[177] 6 U.S.C. § 1503(d)(2).

[178] *Id*. § 1504(b)(3)(B). On February 16, 2016, the DOJ and the Department of Homeland ***security*** issued interim guidelines, as required by the law. U.S. DEP'T OF HOMELAND ***SEC.*** & U.S. DEP'T OF JUSTICE, PRIVACY AND CIVIL LIBERTY INTERIM GUIDELINES (2016), https://www.uscert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.

Cyber Emergency Response Team (ICS-CERT), [179] the FBI works closely with the private sector through its InfraGard program, a public-private partnership with over 30,000 members. The program securely distributes unclassified ***intelligence*** products relating to threats to critical infrastructure and **[*435]** allows affected stakeholders to report incidents directly to the FBI. Furthermore, the FBI has presented over three dozen sector-specific threat briefings to companies in the past year alone. Through such efforts, law enforcement has also attempted to advise private sector actors on the steps they can take to keep their own networks safe. For example, in April 2015, the ***Cybersecurity*** Unit of the Computer Crime and Intellectual Property Section of the Criminal Division released a guidance document advising private companies on best practices for preparing for and responding to ***security*** breaches. [180]

These initiatives capitalize on the comparative advantages of the public and private sectors, while generating the type of persistent coordination required in a threat environment characterized by constantly evolving challenges. The private sector enjoys remarkable expertise, enormous manpower, and an ability to quickly act to protect its own systems. In some cases it also has a technological advantage, at least in relation to monitoring and guarding its own networks. [181] The government has a different kind of expertise, with legal authority to take decisive action and the power to compel cooperation at home using legal process and persuade (or pressure) foreign governments to do the same. In the most important cases, the government can also bring enormous manpower to the table. Together, the private sector and the government each amplifies and strengthens the other, holding out our best chance to disrupt and deter ***cyber*** intrusions before they cause real harm to our economy, our ***security***, and our way of life.

Ultimately, we must find the right balance of industry protections, government action, and civil and regulatory liability--the right combination of carrots and sticks--that incentivizes companies to improve their ***cybersecurity*** without revictimizing them or creating perverse incentives to underreport. Where to strike this balance might change over time. This Article doesn't purport to give the answer. Rather, it sets out a research agenda that will hopefully be taken up by industry and researchers.

Conclusion

We are at the early stages of what will be a long fight against ***national security*** ***cyber*** threats, and DOJ is only beginning to play a significant role in this fight. A good analogy is DOJ's counterterrorism activities shortly after 9/11. Although terrorists had been prosecuted in federal courts before 9/11, the FBI had no ***National Security*** Branch, the ***National Security*** Division hadn't been created, the relationship between foreign ***intelligence*** gathering and law enforcement activities was rapidly transforming, and there were active debates about whether **[*436]** terrorists could be adequately investigated, disrupted, and prosecuted through the domestic criminal justice system. We now use the criminal justice system more

---

[179] Pursuant to EOs 13,636 and 13,691, the Department of Homeland ***Security***'s National ***Cybersecurity*** and Communications Integration Center (NCCIC) collaborates closely with private sector entities to ensure access to classified and unclassified information about ***cyber*** risks and incidents. NCCIC includes US-CERT and ICS-CERT, which together publish hundreds of products each year and provide classified and unclassified briefings.

[180] ***CYBERSECURITY*** UNIT, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF ***CYBER*** INCIDENTS (2015), https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/04/30/04272015reporting-***cyber***-incidents-final.pdf.

[181] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 448-49 (2012).

effectively than ever before in combatting terrorist threats and gaining vital ***intelligence*** on terrorist plots, while at the same time using other tools.

It took multiple years, with occasional course corrections, for the government to develop its strategy--and that strategy is still evolving to meet a changing terrorist threat. Such is the case now with the ***cyber*** threat. The tools described above show great promise, and have already made significant improvements, but they can be used to do more. Prosecutions, takedowns, public attribution, diplomatic and economic pressure--all of these techniques will evolve over the next decade and beyond. And no doubt an article on this subject written ten years from now will highlight tools and activities as yet unimagined.

So although we'll need to race to catch up to today's threat, that will not be enough. The dynamism of the Internet is reflected in the rapidly evolving nature of the ***cyber*** threat: its actors, their motivations, and their tools. The government, and society at large will have to continue to think creatively about how to keep ourselves safe while preserving the dynamism and openness that has made the Internet such a revolutionary invention.

There will be false starts, and even more false peaks. But we must resist cynicism or desperation. Throwing up our collective hands is not an option--not for the engineers who design the technologies and services we use, the public that benefits from them, the academics and researchers who study how to manage these complex systems, and especially not for those tasked with protecting our nation.

Harvard ***National Security*** Journal
Copyright © 2016 President and Fellows of Harvard College. All Rights Reserved.
Harvard ***National Security*** Journal

End of Document

ARTICLE: OBAMA'S NATIONAL SECURITY EXCEPTIONALISM

2016

Reporter
91 Chi.-Kent L. Rev. 91 *

Length: 8934 words

Author: Sudha Setty*

* Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law. The author thanks Raquel Aldana and Jennifer Chacon for their invitation to present this paper during the panel on The Obama Presidency and Rights at the symposium on Congressional Dysfunction and Executive Lawmaking During the Obama Administration held at the 2015 Annual Meeting of the Association of American Law Schools. The author also thanks Matthew H. Charity and Peter Margulies for their thoughtful comments and suggestions. © Sudha Setty 2015.

Text

[*91]

Introduction

One of the premises of this symposium is that the Obama administration, in undertaking various executive actions that protect some of the vulnerable immigrant populations in the United States, is acting in a more rights-protective manner than Congress has explicitly authorized. This Essay juxtaposes this perceived dynamic with policies in the ***counterterrorism*** and ***national security*** realm, areas in which the Obama administration has acted directly in contrast to its more rights-protective stance taken in other areas.

National security is arguably an exceptional context when compared to other issues that touch on domestic and international law and policy, such as immigration. This Essay considers the exceptionalism of Obama administration ***national security*** policies, which have undercut civil and human rights in ways that disparately impact racial and religious minorities. Included in this analysis are the non-prosecution of those who endorsed torture of detainees, use of drones for targeted killings of citizens and noncitizens, invocations of the state secrets privilege, and use of immigration authorities to detain and remove those accused of having a connection with terrorist activity.

The latter part of this Essay situates the Obama administration's ***national security*** policies in the context of this symposium's examination of the horizontal and vertical separation of powers. In doing so, this Essay concludes that the rule of law distortion at both the domestic and international level is enabled by a

pronounced lack of judicial engagement and review of most rights-denigrating ***national security*** **[*92]** programs, political enabling by Congress, and lack of sustained public pressure for reform.

I.

Examples of ***National Security*** Exceptionalism

The label of ***national security*** exceptionalism fits the Obama administration in two ways: first, although the administration has actively sought to address and improve the protection of human rights and civil rights of racial minorities suffering disparate negative treatment in a variety of contexts, those moves toward rights protection generally do not extend to the realm of ***counterterrorism*** abuses. Notably, in the post-***9/11 counterterrorism*** context, almost all of those who have suffered from violations of human and civil rights are racial and/or religious minorities. [1] One of the justifications for this type of exceptionalism is based on the widespread view that ***national security*** is an area in which ordinary legal and constitutional constraints do not apply because of the strong deference that ought to be afforded to the president in foreign policy matters; [2] related to this type of exceptionalism is the outsized perception of the threat of terrorism by politicians and the public, which makes it difficult for the government to shift away from its exceptionalist footing. [3] The second mode of exceptionalism is predicated on the view that the United States plays an **[*93]** exceptional role on the world stage in terms of its responsibility to police global actions by exercising its hard and soft power; as such, it has the right to act in ways that would arguably not be tolerated by the United States if undertaken by a different nation. [4]

---

[1] By "rights protection" in the ***counterterrorism*** context, I mean those actions taken to protect, improve or expand the civil and human rights of those most negatively impacted by the U.S. government's post-September 11, 2001, ***counterterrorism*** policies. Although judges, scholars, and lawyers can argue as to the efficacy and legality of such measures, within the United States, the disparate impact of post-September 11 ***counterterrorism*** laws and policies has been borne heavily by Muslims, Arabs, and people hailing from - or appearing to hail from - South Asia, the Middle East, and North Africa. See, e.g., David Cole, Enemy Aliens, 54 Stan. L. Rev. 953, 957 (2002) (couching the disparate treatment of ***counterterrorism*** policies as falling on Arab noncitizens); Gil Gott, The Devil We Know: Racial Subordination and ***National Security*** Law, 50 Vill. L. Rev. 1073, 1073 (2005) (analyzing how "liberal democratic systems might evolve … to counter the socially and politically pernicious effects of … religiously-inflected, all-or-nothing-warfare"); Natsu Taylor Saito, Beyond the Citizen/Alien Dichotomy: Liberty, Security, and the Exercise of Plenary Power, 14 Temp. Pol. & Civ. Rts. L. Rev. 389, 391-92 (2005) (defining otherness as based on race, national origin, ethnicity, and other factors apart from citizenship); Girardeau A. Spann, Terror and Race, 45 Washburn L.J. 89, 1-02 (2005) (observing that "the sacrifice of racial minority interests for majoritarian gain appears to be an intrinsic feature of United States culture"); Tom R. Tyler et al., Legitimacy and Deterrence Effects in Counter-Terrorism Policing: A Study of Muslim Americans, 44 Law & Soc'y Rev. 365, 366 (2010).

[2] E.g., John Yoo, The Terrorist Surveillance Program and the Constitution, 1714 Geo. Mason L. Rev. 565 (2007) (arguing that ***national security*** surveillance is largely beyond the purview of Congress and the judiciary); Cf. Aziz Huq, Against ***National Security*** Exceptionalism, 2009 Sup. Ct. Rev. 225 (2010) (arguing that, in some cases, the assumption that ***national security***-related cases are treated in an exceptional manner does not bear out).

[3] See Paul Campos, Undressing the Terror Threat, Wall St. J. (Jan. 9, 2010), http://www.wsj.com/articles/SB10001424052748704130904574644651587677752 (arguing that the risk of death from terrorism versus other causes is comparatively infinitesimal, yet government resources are not proportionately allocated); Nate Silver, Crunching the Risk Numbers, Wall St. J. (Jan. 8, 2010), http://www.wsj.com/articles/SB10001424052748703481004574646963713065116 (same as Campos).

[4] President Obama's 2014 commencement address at West Point embodied a variety of arguably complementary, arguably conflicting thoughts on the notion of American exceptionalism. At one point, he noted, "I believe in American exceptionalism with every fiber of my being. But what makes us exceptional is not our ability to flout international norms

A.

Improving Rights Protection in Some Non-security Contexts

Looking at almost seven years of his presidency, it is clear that President Obama has prioritized improving the government's footing on several human and civil rights issues, a number of which have focused on areas in which a racially disparate impact is obvious. For many of these areas, the Obama administration has undertaken its efforts unilaterally, despite a reluctant or sometimes contrary Congress. Immigration is one of these contexts, but other examples reflect presidential efforts toward better protections for racial minorities as well. [5] In the context of voting rights, President Obama immediately pushed back against the Supreme Court's gutting of Section 5 of the Voting Rights Act of 1965 in its Shelby County v. Holder [6] decision of 2013, ordering the Justice Department to continue litigating voting rights cases aggressively and creatively while pushing Congress to **[*94]** restore the protections removed by the Shelby decision. [7] On the issue of racially disparate sentencing for non-violent drug-related crimes, President Obama not only signed the Fair Sentencing Act of 2010 [8] and encouraged the reduction in mandatory minimum sentences, [9] but has also exercised unilateral executive action to encourage those sentenced under the prior racially disparate sentencing framework to seek clemency, [10] and continued to use his clemency power to order the release of some of those convicts. [11] With regard to unarmed racial minorities being harassed, abused, or killed by police, President Obama has spoken out forcefully, moved toward the demilitarization of local

---

and the rule of law, it is our willingness to affirm them through our actions." President Barack Obama, Commencement Address at the United States Military Academy in West Point, N.Y. (May 28, 2014), in U.S. Gov't Publ'g Office, Daily Compilation of Presidential Documents, 2014, at 3, 7. At another point, he offered that "America must always lead on the world stage. If we don't, no one else will," Id. at 3, and continued this theme with the following: The United States will use military force, unilaterally if necessary, when our core interests demand it: when our people are threatened, when our livelihoods are at stake, when the security of our allies is in danger. In these circumstances, we still need to ask tough questions about whether our actions are proportional and effective and just. International opinion matters, but America should never ask permission to protect our people, our homeland, or our way of life. Id.

[5] The following list of activities is meant to be selective, not exhaustive; further, if the scope of analysis were broadened to include issues for which racially disparate impact is not facially obvious, other unilateral rights-protective measures undertaken by the Obama administration could be considered, such as the broadening of workplace, health care, and marital tax filing protections for LGBTQ federal employees.

[6] Shelby County, Ala. v. Holder, 133 S. Ct. 2612 (2013).

[7] See Press Release, White House, President Barack Obama, Statement by the President on the Supreme Court Ruling on Shelby County v. Holder (June 25, 2013) (on file at https://www.whitehouse.gov/the-press-office/2013/06/25/statement-president-supreme-court-ruling- shelby-county-v-holder); see also Jackie Calmes, Obama Reassures Leaders on Enforcing Voting Rights, N.Y. Times (July 29, 2013),http://www.nytimes.com/2013/07/30/us/politics/obama-reassures-leaders-on-enforcing-voting-rights.html (describing conversations among President Obama, Attorney General Holder and civil rights leaders on ways in which the Obama administration would seek to maintain protection of voting rights despite the Shelby ruling).

[8] Fair Sentencing Act 0f 201, Pub. L. No. 111-220, 124 stat 2373, 2374, & 2375.

[9] See Matt Apuzzo, Holder Endorses Proposal to Reduce Drug Sentences in Latest Sign of Shift, N.Y. Times (Mar. 13, 2014), http://www.nytimes.com/2014/03/14/us/politics/holder-endorses-proposal-to-reduce-drug-sentences.html.

[10] See Matt Apuzzo, Justice Dept. Starts Quest to Find Inmates to be Freed, N.Y. Times (Jan. 30, 2014), http://www.nytimes.com/2014/01/31/us/politics/white-house-seeks-drug-clemency-candidates.html.

[11] Michael S. Schmidt, U.S. to Release 6,000 Inmates from Prisons, N.Y. Times (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/us/us-to-release-6000-inmates-under-new-sentencing-guidelines.html (describing plans to commute the sentences of some offenders convicted of non-violent drug-related crimes).

police forces, [12] ordered better training and controls when federal military equipment is transferred to state and local police departments, [13] emphasized the need to improve community policing, [14] and created a task force to "strengthen public trust and foster strong relationships between local law enforcement and the communities that they protect, while also promoting effective crime **[*95]** reduction." [15] In these contexts and others, President Obama has made clear that he intends to use political capital and resources to address some of the civil and human rights challenges in which racial minorities have been negatively impacted by government policies and actions.

B.

Security Contexts with a Mixed Record of Rights Protection

In response to human and civil rights abuses occurring during the George W. Bush administration as a result of ***national security*** and ***counterterrorism*** programs, President Obama initially promised [16] substantial shifts in policy to better protect rights. [17] Although the lofty goals he set forth on the campaign trail in 2008 and early in his administration in 2009 have largely not been met, he has taken some steps to better protect human and civil rights in some areas. Well-known examples include his issuance of executive orders in early 2009 to end the use of torture on detainees [18] and to close the detention facility at Guantanamo Bay, Cuba. [19] These moves toward improved rights protection were laudable, but were

---

[12] See Tonya Somanader, Why President Obama is Taking Steps to Demilitarize Local Police Forces, White House: Blog (May 18, 2015, 7:44 PM), https://www.whitehouse.gov/blog/2015/05/18/why-president-obama-taking-steps-demilitarize-local-police-forces.

[13] See generally Exec. Office of the President, Review: Federal Support for Local Law Enforcement Equipment Acquisition (2014).

[14] Fact Sheet: Strengthening Community Policing, White House (Dec. 1, 2014), https://www.whitehouse.gov/the-press-office/2014/12/01/fact-sheet-strengthening-community- policing.

[15] Fact Sheet: Task Force on 21st Century Policing, White House (Dec. 18, 2014), https://www.whitehouse.gov/the-press-office/2014/12/18/fact-sheet-task-force-21st-century- policing.

[16] President Barack Obama, Inaugural Address, in 1 Pub. Papers, Jan. 20, 2009, at 2. https://www.whitehouse.gov/blog/inaugural-address (rejecting the idea that there must be a trade-off between protection of civil liberties and ***national security***).

[17] The need to increase rights protections in the ***national security*** context operates from the premise that such changes are necessary to comport with the rule of law and human rights law and norms. Many thoughtful scholars have argued that the current structures in place with regard to security policies, such as the use of drones for targeted killing, have achieved a positive, if not ideal, balance of individual rights and security imperatives. See, e.g., Robert M. Chesney, Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force, 13 Yearbook Int'l Humanitarian L. 3 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17 54223 (arguing that the Obama administration has satisfied its international law obligations with regard to the targeted killing of U.S. citizen Anwar al-Awlaki); Matthew Waxman, Going Clear, ForeignPolicy (Mar. 20, 2013), http://www.foreignpolicy.com/articles/2013/03/20/going_ clear (arguing that greater transparency with regard to the drone program may not be an improvement over the current situation); see also Jack Goldsmith, Power and Constraint: The Accountable President After ***9/11*** (2012) (arguing that executive power has been appropriately constrained by various factors in the post-***9/11*** era).

[18] Exec. Order No, 13491 - Ensuring Lawful Interrogations, 74 Fed. Reg. 4893, 4894 (Jan. 22, 2009).

[19] Exec. Order No. 13492 - Review and Disposition of Individuals Detained at the Guantanamo Bay Naval Base and Closure of Detention Facilities, 74 Fed. Reg. 4897, 4898 (Jan. 22, 2009). The Guantanamo Bay detention facility is still

tempered by other **[*96]** policies or aspects of the administration's decision making. In rare instances, the Obama administration has paid compensation to individuals who were abused in some way due to ***national security*** overzealousness during the Bush administration, [20] but this has been more of an exception than the general practice of the administration, which has been to use a variety of tactics to seek dismissal of lawsuits seeking recompense for ***national security*** abuses and to cover up abuses when possible. [21]

For example, despite President Obama's statement affirming the illegality of torture, a continuing United Nations investigation into U.S. torture, [22] and ample evidence made public by the Senate that torture was committed by U.S. government agents under the George W. Bush administration, [23] the Obama administration has made no moves toward seeking accountability for those who authorized, supervised, ordered, or carried out the torture. This is particularly noteworthy in the context of this symposium, which considers whether and the extent to which the Obama administration has gone above and beyond congressional authorization in granting protections and rights to certain immigrants; in the case of torture, we see not only a lack of accountability over the responsible individuals, but also a years-long fight by the Obama administration to keep the detailed findings of the Senate Select Committee on Intelligence secret and out of public **[*97]** view. [24] Where the Senate acted forcefully to detail human rights abuses, the administration continues to remain conspicuously silent as to its obligation to hold perpetrators accountable.

---

open, but the number of detainees has dropped from 242 at the beginning of the Obama presidency to 116 as of summer 2015. See Guantanamo by the Numbers, Human Rights First, http://www.humanrightsfirst.org/sites/default/files/gtmo-by-the-numbers.pdf (last updated Oct. 7, 2015).

[20] In early 2015, the Obama administration settled a lawsuit with Abdullah al-Kidd, who had been detained for sixteen days in 2003 under the federal material witness statute based on gross misrepresentations made by a federal agent on his warrant for detention. As a result of the settlement, al-Kidd was paid $ 385,000 and was issued an apology by the government. See Rebecca Boone, US Citizen Settles Lawsuit Over Post-***9/11*** Arrest with FBI, Seattle Times (Jan. 16, 2015, 3:53 PM), http://www.seattletimes.com/nation-world/us-citizen-settles-lawsuit-over-post-***9-11***-arrest-with-fbi/.

[21] See infra Part 2, Why Not ***National Security*** Exceptionalism?.

[22] The United States has followed up its periodic reports to the UN Committee Against Torture with testimony as to how U.S. policies have changed such that torture is no longer committed in the name of ***national security***, but has not gone further in promising accountability over prior acts of torture. See Tom Malinowski, Assistant Sec'y, State for Democracy, Human Rights and Labor, U.S. Dep't of State, Opening Statement before the United Nations Committee Against Torture (Nov. 12, 2014), on U.S. Mission Geneva, https://geneva.usmission.gov/2014/11/12/malinowski-torture-and-degrading-treatment-and-punishment-are-forbidden-in-all- places-at-all-times-with-no-exceptions/ (last visited Oct. 24, 2015).

[23] See Select Comm. on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, S. Rep. No. 113-288 (2014) [hereinafter Senate torture report] (detailing the many known instances of torture against detainees, as well as the cover up attempted by individuals within the Central Intelligence Agency).

[24] See Connie Bruck, Dianne Feinstein v. the CIA, New Yorker (June 22, 2015), http://www.newyorker.com/magazine/2015/06/22/the-inside-war (detailing the lengthy arguments between Senator Dianne Feinstein, chair of the Senate committee that researched and wrote the Senate torture report, and the administration as to the release of the unclassified portion of the report to the public); Charlie Savage, U.S. Tells Court That Documents From Torture Investigation Should Remain Secret, N.Y. Times (Dec. 10, 2014), http://www.nytimes.com/2014/12/11/us/politics/us-tells-court-that-documents-from-torture-investigation-should-remain-secret.html?_r=0 (describing protracted litigation over FOIA requests for information about the DOJ torture investigation, and administration efforts to keep information secret). See also Dan Froomkin, Holder, Too Late, Calls for Transparency on DOJ Torture Investigation, Intercept (Oct. 15, 2015), https://theintercept.com/2015/10/15/holder-too-late-calls-for-transparency-on-doj-torture-investigation/ (noting that former Attorney General Holder lamented the lack of transparency over the DOJ torture investigation only after he left office).

Statements denouncing torture and promises that this administration will not use such tactics on detainees are better than the Bush administration's actions, but they remain insufficient and the failure to prosecute serious allegations of torture remains in violation of the United States' international obligations.

Another example of the Obama administration's marginal shifts towards rights protection is its movement of some cases from military commissions to Article III courts under the theory that federal courts are an effective venue for prosecutors to secure convictions, and they obviate the rule of law concerns concomitant with the use of specialized military commissions for terrorist acts. [25] Using Article III courts as opposed to military commissions is a shift that moves toward greater rights protection for those on trial, but the reality also includes the fact that federal prosecutors of terrorism acts have the deck stacked in their favor in terms of being able to suspend Miranda rights **[*98]** for a lengthy time, [26] use an extremely broad material support statute to convict or as leverage in plea bargain negotiations, [27] and defend against claims of entrapment with virtually guaranteed success. [28] Despite these significant limitations, some argument can be made that the Obama administration has shifted at least marginally in a rights-protective direction on these matters; the same cannot be said for a number of other ***national security*** contexts.

C.

---

[25] See Eric H. Holder, Jr., Att'y Gen., Speech at the University of California Berkeley School of Law Commencement (May 22, 2013) (transcript at http://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-university-california-berkeley-school-law). Holder noted that: Those who claim that our federal courts are incapable of handling terrorism cases are not registering a dissenting opinion. They are simply wrong. Their assertions ignore reality. And attempting to limit the use of these courts would weaken our ability to incapacitate and to punish those who target our people and attempt to terrorize our communities. Throughout history, our federal courts have proven to be an unparalleled instrument for bringing terrorists to justice. They have enabled us to convict scores of people of terrorism-related offenses since September 11. Id.; see also Sudha Setty, Comparative Perspectives on Specialized Trials for Terrorism,63 Maine L. Rev. 131 (2010) (arguing that the use of military commissions or other specialized terrorism courts is problematic from a rule of law perspective).

[26] See F.B.I. Memorandum, N.Y. Times (Mar. 25, 2011), http://www.nytimes.com/2011/03/25/us/25miranda-text.html (detailing the circumstances under which Miranda warnings can be delayed when interrogating terrorism suspects). This Justice Department policy came under public scrutiny in conjunction with the interrogation of the 2013 Boston marathon bomber, Dzhokhar Tsarnaev, who was detained and questioned for a prolonged period of time before being read his Miranda rights. See Charlie Savage, Debate Over Delaying of Miranda Warning, N.Y. Times (Apr. 20, 2013), http://www.nytimes.com/2013/04/21/us/a-debate-over-delaying-suspects-miranda-rights.html.

[27] See ***Counterterrorism*** Efforts, Offices of the U.S. Att'ys, U.S. Dep't of Justice, http://www.justice.gov/usao/priority-areas/***national-security***/***counterterrorism***-efforts (last updated Dec. 8, 2014) (discussing the importance of the material support statute to federal prosecutors); Wadie E. Said, The Material Support Prosecution and Foreign Policy,86 Ind. L.J. 543 (2011) (critiquing the breadth and vagueness of the material support statute as allowing for too much discretion in prosecuting Muslims with views that are contrary to U.S. foreign policy interests). The material support statute is so useful to prosecutors in the United States that the Department of Justice has provided advice to other nations on how they can import a similar prosecutorial model for domestic use. See Attorney General Holder Urges International Effort to Confront Threat of Syrian Foreign Fighters, Justice News, U.S. Dep't of Justice (July 8, 2014), http://www.justice.gov/opa/pr/attorney-general-holder-urges-international-effort-confront-threat- syrian-foreign-fighters.

[28] See Ctr. on Law & Sec., N.Y. Univ. Sch. of Law, Terrorist Trial Report Card: September 11, 2001-September 11, 2011 26 (2011), http://www.lawandsecurity.org/portals/0/documents/ttrc%20ten %20year%20issue.pdf (noting that post-***9/11*** entrapment defenses in terrorism prosecutions have never been successful); Paul Harris, Fake Terror Plots, Paid Informants: The Tactics of FBI "Entrapment' Questioned, Guardian (Nov. 16, 2011), http://www.theguardian.com/world/2011/nov/16/fbi-entrapment-fake-terror-plots.

Security Contexts in Which Exceptionalism Is at its Highest

Numerous contexts exist in which the Obama administration has either actively undermined attempts at accountability over human and civil rights abuses committed under the auspices of a ***national security*** or ***counterterrorism*** program, or has kept secret the arguably abusive programs in order to shield them from accountability. In this section, three such contexts are discussed: [29] (1) the use of unmanned aerial **[*99]** vehicles (UAVs or drones) for targeted killings, (2) the invocation of the state secrets privilege to seek dismissal of civil lawsuits involving sensitive government information, and (3) the use of immigration law to detain and remove noncitizens accused of a connection to terrorist activity. Each of these embodies at least one aspect of the ***national security*** exceptionalism identified above: that the type of authority claimed by the president is appropriate because it is within his unilateral purview, that terrorism poses an exceptional and unacceptable threat to the United States that must be countered forcefully, and that the United States must play an exceptional role within the ***counterterrorism*** sphere and this role may justify excessive behavior in some instances.

1.

Drones

President Obama expanded the use of drones for targeted killings [30] of suspected terrorists during his administration. [31] Administration officials have repeatedly emphasized the necessity, efficacy, and legality of targeted killings as a ***counterterrorism*** tool, [32] and have resisted the idea that other branches of government should play a significant role over the question of who is killed by drones (citizen vs. noncitizen) and under what circumstances. Nonetheless, the program has prompted much debate over the basic question of whether such a program ought to exist, [33] the moral calculus of extrajudicial killings by remote

---

[29] These three contexts are by no means inclusive of all of the ways in which the Obama administration's ***counterterrorism*** activities have had a disparate negative impact on people who are Muslim, or Arab or South Asian descent, or those perceived to fall into one of those categories. See Sudha Setty, Country Report on ***Counterterrorism***: United States of America, 62 Am. J. Comp. L. 643 (2014) (offering a more comprehensive accounting of the Obama administration's ***counterterrorism*** activities).

[30] Although targeted killing is not defined under international law, it is often considered to encompass "premeditated acts of lethal force employed by states in times of peace or during armed conflict to eliminate specific individuals outside their custody." See Jonathan Masters, Targeted Killings, Council on Foreign Relations (May 23, 2013), http://www.cfr.org/***counterterrorism***/targeted-killings/p9627. Although the governments that utilize targeted killings differentiate them from assassinations, see Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Remarks at the Annual Meeting of the American Society of International Law (Mar. 25, 2010) (transcript at http://www.state.gov/s/l/releases/remarks/139119.htm), critics view them as similar actions in terms of illegality. See, e.g., Complaint at 1, Al-Aulaqi v. Panetta, No. 1:12-cv-01192-RMC (D.D.C. July 18, 2012).

[31] See Drone Database, New Am. Found., http://securitydata.newamerica.net/about.html (last visited Feb. 4, 2014) (detailing the number of drone strikes by the United States in Yemen and Pakistan since 2004).

[32] See Koh, supra note 30, at 7-8.

[33] See, e.g., U.N. Human Rights Council, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Study on Targeted Killings, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) [hereinafter U.N. Human Rights Council] (questioning the legality of the CIA drone program).

control, [34] the legal parameters and authorities for such a **[*100]** program, [35] and specific questions regarding the legality of its scope in terms of geographic location and citizenship of the target. [36] The Obama administration took two positions as to the nature of the war being waged with drones that raised additional concerns: first, the assertion that the theater of war for U.S. ***counterterrorism*** efforts encompasses the entire globe; [37] and second, statements made by administration officials in early 2013 that although the country should not remain on a war footing permanently, we should expect the current ***counterterrorism*** efforts to last at least ten to twenty years longer. [38] Despite the boundless geographic and extremely broad durational scope around the targeted killing program, its parameters remain largely shielded from public view except at points at which it serves the Obama administration to make such information public. [39] Limited information has been disclosed in occasional speeches by **[*101]** administration officials [40] and a classified Department of Justice memorandum that was leaked

---

[34] See generally Samuel Issacharoff & Richard H. Pildes, Drones and the Dilemma of Modern Warfare (N.Y.U. Sch. of Law, Working Paper No. 13-34, 2013) (theorizing the moral dilemma of drone use in the context of warfare in which geographic and other traditional boundaries of violence are distorted).

[35] See U.N. Human Rights Council, supra note 33, at P 28-92 (discussing international law of war principles with regard to targeted killings); Eric H. Holder, Jr., Att'y Gen., U.S. Dep't of Justice, Speech at Northwestern University School of Law (Mar. 5, 2012) (transcript at http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html) (outlining the parameters used by the Obama administration to determine whether a targeted killing comports with international and domestic legal obligations); Jeh C. Johnson, Gen. Counsel, U.S. Dep't of Defense, Speech on ***National Security*** Law, Lawyers and Lawyering in the Obama Administration (Feb. 22, 2012) (transcript at http://www.cfr.org/defense-and-security/jeh-johnsons-speech-***national-security***-law-lawyers-lawyering-obama- administration/p27448) (echoing previous administration legal justifications for targeted killing); Koh, supra note 30, at 7-8 (arguing that the Obama administration's use of targeted killing as a ***counterterrorism*** tool complied with international and domestic legal obligations).

[36] See Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 9, 54 (D.C. Cir. 2010) (dismissing, based on standing grounds, the suit of Nasser al-Aulaqi to enjoin the U.S. government from keeping his son, U.S. citizen Anwar al-Aulaqi, on its targeted killing list).

[37] Spencer Ackerman, Pentagon Spec Ops Chief Sees "10 to 20' More Years of War Against Al-Qaida, wired.com (May 16, 2013, 11:49 AM), http://www.wired.com/dangerroom/2013/05/decades-of-war/ (discussing the Senate testimony of Michael Sheehan, the assistant secretary of defense for special operations and low-intensity conflict, with regard to the global theater of war).

[38] Id. (relating the Senate testimony of Michael Sheehan, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, with regard to the probable duration of the U.S. ***counterterrorism*** effort against al-Qaida).

[39] See David Pozen, The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information, 127 Harv. L. Rev. 512, 625-26 (2013); see, e.g., Stephanie Condon, Obama: Anwar al-Awlaki's Death a "Major Blow" to al Qaeda and Affiliates, CBS News (Sept. 30, 2011, 4:40 PM), http://www.cbsnews.com/news/obama-anwar-al-awlakis-death-a-major-blow-to-al-qaeda-and-affiliates/ (relating comments by President Obama about the strategic importance of the targeted killing Anwar al-Awlaki, an American citizen in Yemen).

[40] E.g., Letter from Eric H. Holder, Jr., Att'y Gen., U.S. Dep't of Justice, to Patrick J. Leahy, Chairman, U.S. Senate Comm. on the Judiciary, in Holder Letter on Counterterror Strikes Against U.S. Citizens, N.Y. Times (May 22, 2013), http://www.nytimes.com/interactive/2013/05/23/us/politics/23 holder-drone-lettter.html?_r=1& (detailing the administration's legal basis for the use of targeted killings against Anwar al-Awlaqi and other U.S. citizens overseas); John O. Brennan, Assistant to the President for Homeland Sec. & ***Counterterrorism***, Remarks of John O. Brennan: Strengthening our Security by Adhering to our Values and Laws (Sept. 16, 2011), http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our- security-adhering-our-values-an; Johnson, supra note 35; Koh, supra note 30, at 7-8.

in early 2013. [41] That leak prompted a May 2013 speech in which President Obama looked to defend the legality of the targeted killings program. [42] At the same time that the administration discussed and leaked aspects of the program, it also used the classified [43] nature of the program to shield itself from media inquiry [44] and from judicial accountability, using the standing doctrine and state secrets privilege to secure the dismissal of a suit challenging the constitutionality of the program. That suit was brought on behalf of U.S. citizen Anwar al-Awlaki, who had been placed on the government's targeted killings list, [45] and who was later killed by a drone. [46] This hypocrisy undermined the credibility of the administration as the restorer of the rule of law and protector of human and civil **[*102]** rights, and instead invited comparisons to the Bush administration that the Obama administration likely wished to avoid for the purposes of garnering domestic and international support. [47]

In his May 2013 speech, President Obama focused largely on the parameters for targeted killings, reiterating known positions of the administration that drone strikes were legal under international law standards [48] because they defended against "imminent" threats, [49] stating that U.S. citizenship is no

---

[41] See U.S Dep't of Justice, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qa'ida or An Associated Force (2011), http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_ DOJ_White_Paper.pdf [hereinafter DOJ White Paper].

[42] See President Barack Obama, Remarks at National Defense University (May 23, 2013), in U.S. Gov't Publ'g Office, 2013, Daily Compilation of Presidential Documents, at 5-6 [hereinafter May 2013 NDU Speech].

[43] See Jo Becker & Scott Shane, Secret "Kill List' Proves a Test of Obama's Principles and Will, N.Y. Times (May 29, 2012), http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?_r=0 (discussing internal administration debates as to whether to declassify the legal justifications for the drone program, and noting that the administration decided not to do so); Charlie Savage, Secret U.S. Memo Made Legal Case to Kill a Citizen, N.Y. Times (Oct. 8, 2011), http://www.nytimes.com/2011/10/09/world/middleeast/secret-us-memo-made-legal-case-to-kill-a-citizen.html (offering details of a still-classified Office of Legal Counsel memorandum justifying the targeted killings of U.S. citizens).

[44] See, e.g., N. Y. Times Co. v. U.S. Dep't of Justice, 915 F. Supp. 2d 508 (S.D.N.Y. Jan. 3, 2013) (dismissing requests made under the Freedom of Information Act for documents regarding the targeted killing program, based on the administration's claim of necessary secrecy surrounding ***counterterrorism*** programs).

[45] See Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010) (dismissing the suit brought by the father of U.S. citizen Anwar al-Awlaki, which sought an injunction against the targeted killing of his son, based on a lack of standing and administration claims of necessary secrecy surrounding ***counterterrorism*** programs).

[46] Anwar al-Awlaki was killed by a drone strike in September 2011. See Charlie Savage, Court Releases Large Parts of Memo Approving Killing of American in Yemen, N.Y. Times (June 23, 2014), http://www.nytimes.com/2014/06/24/us/justice-department-found-it-lawful-to-target-anwar-al-awlaki.html.

[47] See, e.g., Jack Goldsmith, How Obama Undermined the ***War on Terror***, New Republic (May 1, 2013), www.newrepublic.com/article/112964/obamas-secrecy-destroying-american-support-***counterterrorism*** (arguing that Obama's lack of transparency on drones and other issues has undermined U.S. efforts to build alliances that would bolster U.S. foreign policy and ***counterterrorism*** goals).

[48] Compare May 2013 NDU Speech, supra note 42, at 5, with Holder, supra note 35, and Koh, supra note 30, at 7-8 (President Obama articulated proportionality and distinction principles that largely reflected the standards offered by Attorney General Holder and State Department Legal Adviser Koh in previous speeches).

[49] May 2013 NDU Speech, supra note 42, at 6 (articulating similar definitions as to the "imminence" of a perceived threat for the purposes of ordering a targeted killing).

protection against being targeted for a drone strike, [50] and making clear that he could keep as much of the drone program secret as he deemed. [51] Throughout the Obama presidency, the administration has offered only two rights-protective concessions with regard to the drone program, and neither provides significant comfort: first, in 2013, President Obama announced a plan to curtail sharply the use of signature strikes [52] in Yemen and instead use drone strikes only for those individuals targeted by the administration, [53] likely in response to media coverage of tragic civilian deaths [54] and criticism over administration prevarications as to how **[*103]** many civilians had been killed by drone strikes. [55] However, in the first half of 2015, the administration had used signature strikes in Yemen at least twelve times. [56] Second, in 2013, then-Attorney General Eric Holder conceded to Senator Rand Paul that the president does not have the authority to use a weaponized drone to kill an American not engaged in combat on American soil, [57] apparently leaving open the possibility of noncitizens being killed anywhere, U.S. citizens being killed outside of the United States, and U.S. citizens being killed within the United States if the administration believes that they are engaged in "combat."

Given the boundless geographic scope and lengthy predicted duration of this conflict, alongside the administration's robust defense of both the effectiveness and legality of the program, it would seem that instituting proper accountability measures - by Congress and/or the judiciary - would be essential to protect against and provide redress for arbitrary or abusive decision-making in the process of extra-judicial killings. Yet this area persists as one in which ***national security*** exceptionalism has prevailed. Congress has

---

[50] Compare id., supra note 42, at 8 (noting that "the high threshold that we've set for taking lethal action applies to all potential terrorist targets, regardless of whether or not they are American citizens"), with Holder, supra note 35, at 6.

[51] See May 2013 NDU Speech, supra note 42, at 7, 10.

[52] See Becker & Shane, supra note 43 (explaining that the Obama administration used "signature strikes" in Pakistan, in which groups of people engaging in apparently suspicious behavior were allowed to be targeted for a drone strike, even if no terrorists or terrorist supporters were known to be in the group).

[53] See May 2013 NDU Speech, supra note 42, at 4-5.

[54] See, e.g., Becker & Shane, supra note 43 (discussing a 2009 drone strike that "killed not only its intended target, but also two neighboring families, and left behind a trail of cluster bombs that subsequently killed more innocents… . Videos of children's bodies and angry tribesmen holding up American missile parts flooded YouTube, fueling a ferocious backlash that Yemeni officials said bolstered Al Qaeda"); Eye of the Drone, Harper's Mag. (June 2012), http://harpers.org/archive/2012/06/eye-of-the-drone/ (describing those killed by a drone strike in a Pakistani village and the reluctance of families to congregate for fear of being killed by drones).

[55] See Scott Shane, C.I.A. is Disputed on Civilian Toll in Drone Strikes, N.Y. Times (Aug.11, 2011), http://www.nytimes.com/2011/08/12/world/asia/12drones.html (relating evidence from various sources that the civilian toll of drone strikes was significantly higher than the C.I.A. had claimed); Micah Zenko, Why Won't the White House Say How Many Civilians Its Drones Kill?, Atlantic (June 5, 2012, 8:45 AM), http://www.theatlantic.com/international/archive/2012/06/why -wont-the-white-house-say-how-many-civilians-its-drones-kill/258101/ (noting that John Brennan affirmed in 2011 that "there hasn't been a single collateral death because of the exceptional proficiency, precision of the capabilities we've been able to develop"); see also Becker & Shane, supra note 43 (noting that the C.I.A. had previously counted all military-age males killed by drone strikes as combatants, thereby drastically reducing the number of individuals possibly counted as part of the civilian death toll).

[56] See Greg Miller, CIA Didn't Know Strike Would Hit al-Qaeda Leader, Wash. Post (June 17, 2015), https://www.washingtonpost.com/world/***national-security***/al-qaedas-leader-in-yemen-killed-in-signature-strike-us-officials-say/2015/06/17/9fe6673c-151b-11e5-89f3-61410da94eb1_story.html.

[57] Letter from Eric H. Holder, Jr., Att'y Gen., U.S. Dep't of Justice, to Senator Rand Paul, Paul.Senate.Gov (Mar. 7, 2013) (on file at http://www.paul.senate.gov/files/documents/WhiteHouseLetter.pdf).

expressed little will in setting meaningful parameters on the program, [58] and the judiciary has shied away from adjudicating the legality of placing targets for extrajudicial killings on a government list, even if those targets are U.S. citizens who are not "imminently" attacking the United States in any conventional sense of the word. [59] Actual protection of rights **[*104]** would necessitate more than rhetoric about the efficacy and legality of the drone program that cannot actually be examined and verified because of executive branch secrecy. [60]

2.

State Secrets Privilege

Focus on invocations of the state secrets privilege ramped up during President Bush's second term with the emergence of a pattern of the administration seeking dismissals of lawsuits during the pleadings stage, even when the suits dealt with allegations of extraordinary rendition, unlawful detention ***and torture, and*** the suits were the last attempts of gravely injured individuals to vindicate their rights. [61] Despite substantial evidence that citizens of Germany [62] and the United Kingdom, [63] among others, were rendered by the United States government to other nations and were subsequently abused by the security forces in the nations to which they were rendered, their civil suits have been dismissed on state secrets grounds. [64] Congress discussed reining in the executive's increasing reliance on the state secrets privilege as a means of escaping the possibility of accountability several times: it debated the State Secrets Protection Act of

---

[58] To date, Congress has not taken any action on curbing the Obama administration's use of drones for targeted killings. Administration lawyers have taken the position that disclosure to, consultation with, or approval from Congress is unnecessary and unwarranted with regard to drone strikes. See DOJ White Paper, supra note 41.

[59] See Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 54 (D.D.C. 2010).

[60] Leaking of government information continues to be the primary method by which the media, the public and Congress has been able to prompt further government disclosures about the drone program. In October, 2015, the Intercept media organization used leaked information to report on numerous aspects of the U.S. targeted killing program. See The Drone Papers, Intercept, https://theintercept.com/drone-papers (last visited Oct. 24, 2015). As of this writing, the U.S. government has not issued a response.

[61] Press Release, Office of Sen. Edward M. Kennedy, Sen. Kennedy Introduces State Secrets Protection Act (Jan. 22, 2008) (internal quotation marks omitted), in NewsRoom, 2008 WLNR 1256008; William G. Weaver & Robert M. Pallitto, State Secrets and Executive Power, 120 Pol. Sci. Q. 85, 109 (2005) (claiming that the Bush administration is using the state secrets privilege with "offhanded abandon"); cf. Robert M. Chesney, State Secrets and the Limits of ***National Security*** Litigation, 75 Geo. Wash. L. Rev. 1249, 1252 (2007) (claiming that a survey of the invocation of the state secrets privilege since the 1950s indicates that "recent assertions of the privilege are not different in kind from the practice of other administrations").

[62] See Jane Mayer, The Dark Side: The Inside Story of How the ***War on Terror*** Turned into a War on American Ideals 282-87 (2008) (detailing Khalid El-Masri's plight).

[63] See Sudha Setty, Judicial Formalism and the State Secrets Privilege, 38 Wm. Mitchell L. Rev. 1630, 1634-35 (2012) (detailing the claims of Binyam Mohamed).

[64] E.g., Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1092-93 (9th Cir. 2010) (en banc); El-Masri v. United States, 437 F. Supp. 2d 530, 539 (E.D. Va. 2006), aff'd, 479 F.3d 296 (4th Cir. 2007), cert. denied, 128 S. Ct. 373 (2007).

2008 [65] and reintroduced nearly identical reform legislation in February **[*105]** 2009 [66] after the Obama administration appeared to adopt the Bush administration's stance in favor of a broad invocation and application of the privilege. [67]

Legislative reform efforts lost momentum after the Obama administration released a new policy for the Department of Justice in September 2009 that mandated a more rigorous internal administrative review prior to invoking the state secrets privilege. [68] That policy has been in effect for six years, but it appears that the internal review process has resulted in little visible difference between the Bush and Obama administrations with regard to the invocation of the privilege at the pleadings stage in cases that often allege serious constitutional violations and human rights abuses. [69] More rigorous due process within the executive branch may indeed be more rights-protective, but because such evaluations have been kept secret and Congress and the public are not privy to that information, it appears that the Obama administration has adopted the "just trust us" view of due process that in some respects mirrors the actions of the Bush administration. [70] Further, any future administration could easily undo any rights-protective due process measures that do exist, since the current process was not undertaken legislatively and does not engage Congress or the judiciary in a meaningful way.

The use of the state secrets privilege becomes a matter of ***national security*** exceptionalism because, as in the case of torture, the **[*106]** Obama administration has suppressed the ability of individuals to litigate their rights and hold government actors accountable for their past abuses. Further, a variety of political and structural incentives have created a situation where exceptionalism reigns and accountability from Congress or the courts does not exist: ideological alignment with the president, concern that ***national security*** is an issue within the president's sole jurisdiction, complacency, and an overly formalistic judiciary that chooses to defer to the president instead of engaging in its counter majoritarian obligation to protect

---

[65] 154 Cong. Rec. S198-201 (daily ed. Jan. 23, 2008) (statement of Sen. Kennedy on the State Secrets Protection Act).

[66] See Press Release, Office of U.S. Sen. Patrick Leahy, Leahy, Specter, Feingold, Kennedy Introduce State Secrets Legislation (Feb. 11, 2009) (on file at http://www.leahy.senate.gov/press/press_releases/rele ase/?id=81a196e2-692e-498d-bf80-96ba81e252b5).

[67] Editorial, Continuity of the Wrong Kind, N.Y. Times (Feb. 11, 2009), http://www.nytimes.com/2009/02/11/opinion/11wed2.html (disagreeing with the Obama administration's decision to continue the Bush administration invocations of the state secrets privilege to try to have litigation against the government dismissed at the pleadings stage).

[68] See Memorandum from Eric H. Holder, Jr., Att'y Gen., U.S. Dep't of Justice, to Heads of Exec. Dep'ts & Agencies, Policies and Procedures Governing Invocating of the State Secrets Privilege (Sept. 23, 2009) (on file at http://legaltimes.typepad.com/files/ag-memo-re-state-secrets-dated-09-22-09.pdf) [hereinafter Holder Memorandum] (establishing layers of internal review within the Department of Justice and including a new executive branch policy to report to Congress any invocations of the state secrets privilege).

[69] See Sudha Setty, Litigating Secrets: Comparative Perspectives on the State Secrets Privilege, 75 Brook. L. Rev. 201, 257-58 (2009) (identifying the continuity between the Bush and Obama administrations in their approach to the state secrets privilege).

[70] Most recently, the Obama administration invoked the state secrets privilege as a third party in a defamation suit, securing dismissal without disclosing to either party the basis on which the privilege was invoked. See US Government Invokes State Secrets Privilege to Have Iran Lawsuit Thrown Out, Guardian (Mar. 23, 2015), http://www.theguardian.com/world/2015/mar/23/us-government-lawsuit-iran-state-secrets.

fundamental rights [71] have all contributed to the lack of engagement on the question of redress for violations of human and civil rights.

3.

Use of Immigration Law in the ***National Security*** Context

The government has, to some extent, conflated immigration and ***counterterrorism*** programs and has encouraged use of the immigration system as an important tool in ***counterterrorism*** efforts. [72] The result has been a system that, although legal under U.S. domestic law, [73] arguably violates international law and norms with regard to the treatment of migrants, [74] and most certainly is not rights-protective of the noncitizens caught in its framework. Juxtaposed against the unilateral executive action that has attempted to offer additional protection to some immigrant populations that is the subject of other articles in this symposium, the administration has leveraged the lowered due process protections afforded to immigrants to conduct heightened surveillance, engage in racial and religious profiling, and detain and remove immigrants on a sometimes specious basis.

The government is authorized to detain any person for whom it has certified that reasonable grounds exist to believe that the person **[*107]** has engaged in espionage, [75] opposition by violence, [76] or terrorist activity, [77] or is involved with an organization that is suspected of terrorist activity. [78] Since September 11,

---

[71] See generally Setty, supra note 63 (discussing the overly formalistic approach of the judiciary with regard to government invocations of the state secrets privilege).

[72] See, e.g., John Ashcroft, Att'y Gen., & James W. Ziglar, Comm'r, Immigration & Naturalization Serv., Announcement of INS Restructuring Plan (Nov. 14, 2001) (transcript at http://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks11_14.htm ("The INS will also be an important part of our effort to prevent aliens who engage in or support terrorist activity from entering our country.").

[73] See Office of Inspector Gen., Dep't. Of Homeland Sec., OIG-11-81, Supervision of Aliens Commensurate with Risk 1 (2011) [hereinafter DHS 2011 IG Report] (noting that immigration authorities had generally complied with applicable domestic laws).

[74] See Ctr. for Human Rights and Global Justice, Asian Am. Legal Def. & Educ. Fund, Under the Radar: Muslims Deported, Detained, and Denied on Unsubstantiated Terrorism Allegations 18 (2011), http://aaldef.org/UndertheRadar.pdf [hereinafter Under the Radar) (citing the conclusion of the U.N. Special Rapporteur on the Rights of Migrants that U.S. immigration enforcement policies violate international laws that bar arbitrary detention).

[75] Immigration and Nationality Act (INA) § 237(a)(4)(A)(i), 8 U.S.C. § 1227(a)(4)(A)(i) (2012) (authorizing detention for those suspected of engaging in espionage, sabotage, or export control).

[76] 8 U.S.C. § 1227(a)(4)(A)(iii) (authorizing detention for those expressing opposition by violence or overthrow of the U.S. government).

[77] INA § 212236(a), 8 U.S.C. § 1226(a) (2012) (authorizing detention for those suspected of terrorist activity); 8 U.S.C. § 1182(a)(3)(B)(i)(III), (iv)(I) (2012) (authorizing removal of those indicating an intention to cause death or serious bodily harm or have incited terrorist activity); 8 U.S.C. § 1182(a)(3)(B)(i)(VIVII) (making inadmissible aliens who endorse or espouse terrorist activity or persuade others to endorse or espouse terrorist activity).

[78] See 8 U.S.C. § 1182(a)(3)(B)(vi)(II)-(III); see also U. N. Sec. Council, Letter dated June 15, 2006 from the Chairman of the Security Council Committee Established Pursuant to Resolution 1373 (2001) Concerning Counter-terrorism addressed to the President of the Security Council, U.N. Doc. S/2006/397 (June 16, 2006) (noting that "if a group is designated or treated as a terrorist organization...[for immigration purposes,] aliens having certain associations with the

2001, the federal government has relied heavily on immigration law and policy to detain, interrogate, control and remove suspected terrorists. [79] With fewer checks and balances, it is much easier for the government to arrest, detain, and investigate an individual under immigration law than criminal law. Unlike the U.S. criminal justice system, where defendants have the right to an attorney, the right to a speedy trial, and the presumption of innocence until guilt is proven beyond a reasonable doubt, immigration law does not afford detainees ample protections. For example, a noncitizen is permitted to have an attorney in immigration proceedings, but counsel is not provided for the 80% of detainees in removal proceedings who are indigent. [80] Furthermore, a noncitizen can be mandatorily detained for months or years before being released or removed from the United States, and the standard for removal is that of "clear and convincing evidence," a much lower standard than the criminal justice conviction standard of beyond a reasonable doubt. [81]

These lesser protections have allowed federal officials to undertake several initiatives that have targeted immigrants, primarily those from Muslim-majority countries, in the name of ***national security***. MusHD **[*108]** lims in the immigration system have been subjected to possibly abusive [82] preventive detention, [83] exclusion based on political views, heightened surveillance and arguably unconstitutional racial profiling. [84] Detainees in the immigration system face serious hurdles in challenging the government's case for removal due to the lower removal standard of "clear and convincing evidence" as well as the inability to access and challenge the secret evidence presented and alleged by the government. [85]

Additionally, the Federal Bureau of Investigation (FBI)'s police powers have generated a high level of scrutiny and surveillance of immigrant populations within the United States. The lowered due process protections accorded to immigrants allow for a more searching and less privacy-protective approach. Lawyers cite the presence of FBI agents during immigration proceedings, Immigration and Custom Enforcement's reliance on statements made in old FBI interviews in its decisions, and the FBI's submission of prejudicial affidavits raising ***national security*** concerns without providing the basis of the allegations.

---

group (including persons who knowingly provide material support to the group) become inadmissible to and deportable from the United States.").

[79] In 2009, Immigration and Customs Enforcement (ICE) had over 1.6 million aliens in its scope of monitoring: in ICE detention centers, in other jails or prisons, or under a released monitoring system. See DHS 2011 IG Report, supra note 73, at 3.

[80] See Under the Radar, supra note 74, at 3.

[81] 8 U.S.C. § 1229a(c)(3)(A).

[82] See Ashcroft v. Iqbal, 556 U.S. 662, 667-69 (2009).

[83] Another category of detained aliens are those subject to an additional interagency screening called, Third Agency Check. This system to screen aliens in ICE custody who are from specially designated countries (SDCs) that have "shown a tendency to promote, produce, or protect terrorist organizations or their members." See DHS 2011 IG Report, supra note 73, at 5. The SDC list is largely comprised of majority Muslim nations. See ICE List of Specially Designated Countries (SDCs) that Promote or Protect Terrorism, public intelligence (July 2, 2011), http://publicintelligence.net/specially-designated-countries/.

[84] See Under the Radar, supra note 74, at 4 (discussing various programs targeting noncitizens, including Absconder Apprehension Initiative, NSEERS special registration policy, and Operation Frontline). Another controversial immigration policing program is Secure Communities, which requires state and local police to send fingerprints of arrestees to ICE so that undocumented immigrants can be identified and possibly detained, prosecuted and removed. See Secure Communities, U.S. Immigration & Customs Enf't, U.S. Dep't of Homeland Sec., http://www.ice.gov/secure_communities/ (last visited Nov. 9, 2015) (describing the Secure Communities program).

[85] See Under the Radar, supra note 74, at 3, 4.

FBI agents have used the structural power imbalances inherent in the immigration processes to coerce Muslim immigrants into becoming informants, or retaliate if they refuse. [86]

II.

Why Not ***National Security*** Exceptionalism?

The preceding section offered both the rationales for ***national security*** exceptionalism and several examples of it. The next question must then be, why not stick with ***national security*** exceptionalism? Beyond President Obama's exhortations that ***national security*** ought not **[*109]** be an exceptional context, the focus here should be on the compelling problem of a lack of accountability over the commission of human and civil rights abuses. Both legal and pragmatic problems arise by categorizing ***national security*** matters as being fundamentally separate from other areas in which the administration has worked to protect or improve human and civil rights.

For example, the United States has long been party to international treaties prohibiting torture and cruel, degrading, and inhuman treatment, as well as extra-judicial killing and the disparate treatment of individuals based on race, ethnicity, and religious expression. Among them are the Universal Declaration of Human Rights, [87] the Geneva Conventions, [88] the International Covenant on Civil and Political Rights, [89] the American Convention on Human Rights, [90] and the Convention Against Torture. [91] On the domestic level, the Fifth, Eighth and Fourteenth Amendments to the U.S. Constitution have been interpreted as prohibiting torture, [92] and various domestic laws codify the obligations in the Convention Against Torture: the federal Torture Statute, [93] the Torture Victim Protection Act of 1991, [94] the Alien Tort Claims Act, [95] and the Foreign Affairs Reform and Restructuring Act of 1998. [96] There are no loopholes in international and domestic law that allow for torture, even in times of emergency. Further, international law demands that government-sanctioned torture must be investigated and prosecuted where found. The exceptionalism for the Bush administration was redefining the underlying acts so as to claim **[*110]** that whatever techniques

---

[86] See id. At 8.

[87] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[88] Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

[89] International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171.

[90] American Convention on Human Rights, O.A.S. Treaty Series No. 36, July 18, 1978, 1144 U.N.T.S. 123.

[91] U. N. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, 1465 U.N.T.S. 85.

[92] See generally Seth F. Kreimer, Too Close to the Rack and the Screw: Constitutional Constraints on Torture in the ***War on Terror***, 6 U. Pa. J. Const. L. 278 (2003).

[93] Foreign Relations Authorization Act of 1994, Pub. L. No. 103-236, § 506, 108 Stat. 382 (codified at 18 U.S.C. §§2340-2340B (2006)).

[94] Torture Victim Protection Act of 1991, Pub. L. No. 102-256, 106 Stat. 73 (codified at 28 U.S.C. § 1350)).

[95] Alien Tort Claims Act, 28 U.S.C. § 1350.

[96] Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. No. 105-277, § 2242(a), 112 Stat. 2681 (codified at 8 U.S.C. § 1231 (2006)).

were being used by interrogators on detainees did not constitute torture. [97] For the Obama administration, the exceptionalism was deciding that, despite international law obligations to the contrary, the administration would not conduct an investigation into Bush-era torture [98] and ultimately would not prosecute any of those involved. [99] The administration has remained steadfast in this position despite the evidence made public through the Senate Torture Report, [100] and has aggressively sought dismissal of civil suits alleging torture, as described above.

For targeted killings, the international legal standards are murkier. The Obama administration's stated limits on the use of drones reflect a unilateralist legal interpretation of the applicable international and domestic legal constraints; as with much of the ***counterterrorism*** power that has aggregated in the executive branch since September 2001, there is no venue for challenging the administration's legal position other than through public pressure. [101] In his May 2013 speech, **[*111]** President Obama stated that he welcomed a conversation with Congress about a potential drone court, but noted that, given the scope of executive power in the area of foreign policy and ***counterterrorism***, such a court may not be constitutional. [102] Such a view provides little more than cold comfort to those seeking to protect the rights of citizens and noncitizens being targeted for extrajudicial killings in the name of ***counterterrorism***.

For these contexts, exceptionalism cannot be justified from a purely legal perspective, so the fallback justification turns on pragmatic concerns such as whether the administration thinks particular actions - like targeted killings or the non-prosecution of those involved in torturing detainees - benefit U.S. security interests or make sense from the perspective of political viability. And in this respect, President Obama is

---

[97] Memos prepared by the Office of Legal Counsel in 2002 and 2003 advised the President and the military that detainees who were suspected members of Al Qaeda were not protected by international and domestic prohibitions against torture and, furthermore, that abuse of detainees would not constitute "torture" unless the interrogators intended to cause the type of pain associated with death or organ failure. See Memorandum from Jay S. Bybee, Asst. Att'y. Gen., to Alberto R. Gonzales, Counsel to the President, Standards of Conduct for Interrogation Under 18 U.S.C. §§2340-2340A (Aug. 1, 2002); Memorandum from Jay S. Bybee, Asst. Att'y. Gen., to John Rizzo, Acting Gen. Counsel of the Cent. Intelligence Agency, Interrogation of al Qaeda Operative (Aug. 1, 2002). Those memos were subsequently rescinded, and several members of the military were convicted at courts-martial for detainee abuse. See Scott Shane et al., Secret U.S. Endorsement of Severe Interrogations, N.Y. Times (Oct. 4, 2007), http://www.nytimes.com/2007/10/04/washington/04interrogate.h tml?pagewanted=all.

[98] David Johnston & Charlie Savage, Obama Reluctant to Look into Bush Programs, N.Y. Times (Jan. 11, 2009), http://www.nytimes.com/2009/01/12/us/politics/12inquire.html (noting President Obama's statement that "we need to look forward as opposed to looking backwards").

[99] Scott Shane, No Charges Filed on Harsh Tactics Used by the C.I.A., N.Y. Times (Aug. 30, 2012), http://www.nytimes.com/2012/08/31/us/holder-rules-out-prosecutions-in-cia-interrogations.html.

[100] Jennifer Bendery & Ali Watkins, Despite Torture Uproar, DOJ Still Says No to Prosecutions, Huffington Post (Dec. 9, 2014), http://www.huffingtonpost.com/2014/12/09/doj-torture_n_6298276.html.

[101] For comprehensive treatment of the aggregation of presidential ***counterterrorism*** power in during the Bush administration, see generally Jack Goldsmith, The Terror Presidency (2009) (addressing the problematic aggregation of executive power during the Bush administration); Frederick A.O. Schwarz Jr. & Aziz Z. Huq, Unchecked and Unbalanced: Presidential Power in a Time of Terror (2007) (same). For similar assessments of presidential power during the Obama administration, see generally Afsheen John Radsan, Bush and Obama Fight Terrorists Outside Justice Jackson's Twilight Zone, 26 Const. Comment. 551 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=16 84720; Aziz Rana, Responses to the Ten Questions,37 Wm. Mitchell L. Rev. 5099 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=21 93084.

[102] See May 2013 NDU Speech, supra note 42, at 8.

unexceptional; many presidents have used these pragmatic, non-legal justifications for their ***national security*** actions. Perhaps the only thing exceptional about this situation is that President Obama had promised a return to a non-emergency footing for the government and a return of the primacy of the rule of law.

Conclusion

Some parts of President Obama's ***national security*** exceptionalism should not be surprising; he advertised as early as his first presidential campaign that, if elected, he would send drones into Pakistan to target individuals there. [103] Yet his shift on the issues identified here have created two problematic dynamics with regard to rights protection: first, President Obama's rhetoric about restoring the rule of law and curtailing the perceived abuses of executive power [104] arguably could have translated into meaningful reform that differentiated the Obama administration from the Bush administration's approach on the exercise of unilateral executive power. [105] But repeated invocations of broad executive power and the excessive secrecy that has **[*112]** surrounded many of the Obama administration's policies, combined with excessive deference from the judiciary [106] and a lack of action in Congress on many of these matters, has essentially given a bipartisan imprimatur to claims of extremely broad executive power, a lack of rights-protective action on behalf of those subject to unfair disparate impact by the government, and a lack of accountability for past abuses.

Second, this exceptionalism has taken and continues to take a toll on the view of the United States in the international sphere. Even before he became president, Obama signaled the desire to reengage with the international community as a matter of legal compliance (e.g., outlawing the use of so-called "enhanced interrogation techniques"), [107] as good foreign policy (i.e., restoring America's moral authority in the world) [108] and as a matter of restoring the rule of law. [109] At least since 2009, the U.S. government has looked to garner the support and loyalty of allied nations that were skeptical of Bush-era U.S. ***counterterrorism***

---

[103] E.g., Presidential Debate Transcript, Sept. 26, 2008, MSNBC (Oct. 2, 2008), http://www.nbcnews.com/id/26990647/ns/politics-the_debates/t/presidential-debate-transcript- sept/#.VbeeCvlcCSo.

[104] See Editorial, Mr. Obama and the Rule of Law, N.Y. Times (Mar. 21, 2009), http://www.nytimes.com/2009/03/22/opinion/22sun1.html (detailing the ways in which the Obama administration had already deviated from campaign promises to curtail executive power and restore the rule of law with regard to ***national security*** policies).

[105] See Sudha Setty, No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win, 57 Kan. L. Rev. 579, 596-98 (2009) (discussing the ways in which the Bush administration employed a unilateralist unitary executive theory of power with regard to ***national security***).

[106] See Setty, supra note 63, at 1633-39 (detailing the overly deferential attitude of courts to invocations of the state secrets privilege by the Obama administration).

[107] See Exec. Order No. 13491 - Ensuring Lawful Interrogations, 74 Fed. Reg. at 4893-94 (reiterating the international and domestic law parameters for interrogations of detainees suspected of terrorist activity).

[108] Obama: "We've Restored America's Standing', CNN (Nov. 18, 2009, 10:03AM), http://www.cnn.com/2009/POLITICS/11/18/obama.henry/ (President Obama describing the ways in which the global community has improved its impression of United States foreign policy in the time since he took office).

[109] Adam Cohen, Democratic Pressure on Obama to Restore the Rule of Law, N.Y. Times (Nov. 14, 2008), http://www.nytimes.com/2008/11/14/opinion/14fri4.html.?pagew anted=print&_r=0 (noting that Democratic legislators were planning to hold then President-Elect Obama to his campaign promises to restore the rule of law).

efforts perceived to be dismissive of the countries' own priorities and cultural norms. [110] President Obama's signing of the executive orders outlawing torture and closing the Guantanamo Bay detention facility on his first day in office were meant as strong signals that the U.S. government was responding to concerns that the United States flouted its own human rights standards, disregarded the rule of law, and lacked sensitivity to Muslims around the world. These **[*113]** changes have served not only moral interests, but the realpolitik interests of rebuilding trust and loyalty from traditionally-allied nations. [111]

But continued ***national security*** exceptionalism engenders a view of the United States as considering itself to be above international obligations to investigate and prosecute torturers and war criminals, and the view by the global community that the United States is willing to apply one standard for itself, and another for the rest of the world. As such, the exceptionalism not only poses real challenges in terms of law, morality and building useful relationships with allied nations, but it acts as a step backward for the creation of enforceable international norms and standards, and a step backward in efforts to restore a balance in the rule of law when it comes to ***national security*** matters.

Chicago-Kent Law Review
Copyright (c) 2016 Chicago-Kent College of Law
Chicago-Kent Law Review

End of Documen

[110] See Brennan, supra note 40 (stating that maintaining strong alliances through upholding the rule of law was imperative).

[111] Sudha Setty, ***National Security*** Interest Convergence, 4 Harv. Nat'l Sec. J. 185, 212 (2012).

THE ATTACK ON THE CAPITOL CALLS FOR A MEASURED RESPONSE

EMILY BERMAN*

There are many indisputable facts about violent and deadly incursion into the Capitol building on January 6th. It is beyond debate that the fiasco included multiple criminal acts. Nor is there any question that it represents a colossal security failure on the part of those whose mission is to safeguard the premises and the people inside. Finally, as many observers have noted, the differential treatment afforded to the largely White crowd of President Donald Trump's supporters compared to the Black Lives Matter protestors who took to the streets this summer to protest acts of police violence against Black individuals was, to say the least, stark. Each of these facts—the criminal acts, the security failure, and the differential treatment afforded to those protesting—demand thorough investigation and a vigorous response. But that response need not—indeed *must* not—include measures that ultimately repress peaceful protest and restrict the right to assembly for Americans of all political stripes.

Take first the criminal activity. The crimes that were committed in and around the Capitol Building on Jan. 6 should be investigated and prosecuted. Fortunately, federal prosecutors have no lack of tools at their disposal to address the lawless activity. As others have documented, the list of offenses depicted in images and videos from both inside and outside the Capitol is extensive. They range from the relatively minor offense of trespassing to the possibility of seditious conspiracy. Rather than focusing on the existing laws that were broken, however, much commentary has sought to use the incident as justification for enacting a new law against domestic terrorism. While such a law might be intended to deter white supremacist terrorism, it will inevitably be used against those communities that most frequently cross paths with law enforcement. To be sure, anyone who planted a bomb likely committed a terrorist act. But such actions already are subject to significant penalties, and to depict the entire crowd as "terrorists," or even "rioters," (though surely some individuals present were guilty of that offense as well) is simply to paint with too broad a brush. Assigning collective guilt to an entire crowd due to the actions of a (perhaps significant) minority of those present simply criminalizes the First Amendment protected right to express dissent. By all means, prosecute the criminals, demonstrate that violence is not a valid tool of political dissent. But don't place non-violent protestors on the "No Fly" list or allow righteous outrage at the sacking of the Capitol become a weapon to be employed against the very democratic values that building represents.

This risk is not limited to the federal level. In recent years, many local and state governments have introduced or enacted new laws to deter lawful protests against, for example, petrochemical companies or oil pipelines. These measures impose enhanced penalties for already prohibited activity, such as trespassing or obstructing traffic, when they occur in the context of a peaceful demonstration. The result is criminalization of protest itself. Analogous measures proposed in the wake of the events of Jan. 6th are similarly problematic. Understanding the government's incentives to suppress the voices of its critics, the Constitution builds a buffer around free speech rights, limiting criminal liability for expressing ideas to actual acts of violence or incitement to violence. Any efforts to encroach on this buffer in response to expression we might find odious or ideas we might deem illegitimate renders more fragile the right to expression in all its forms.

Second, the Capitol Police's failure to preserve the security of the Capitol Building and those within it should be studied, and appropriate reforms put in place. What happened was an avoidable and dangerous failure to adequately prepare for or respond to exceptionally predictable behavior. But this failure also risks prompting a significant overreaction. The tableau of Americans coming to petition for redress of their grievances at the seat of government is a fundamental symbol of American democracy. Yet for President Biden's inauguration Washington D.C. was transformed into a fortress guarded by tens of thousands of armed individuals, and the new fence erected around the Capitol grounds—similar to the one that recently turned Lafayette Square "from a public square to a fortress"—is set to remain there until at least the end of January. As a temporary matter, these measure may be justified by the reported plans for additional, potentially violent gatherings cited by Twitter as justification for its permanent suspension of President Trump's account and the need to secure the city for Presidential inauguration. But to turn Capitol Hill into a fortified bunker from which the American people are excluded would not only send an anti-democratic message both domestically and to the rest of the world, but would itself serve to significantly undermine First Amendment values. As soon as it is safe to do so, the extra fortification of the Capitol, already a highly securitized space, should come down.

Finally, the contrast between law enforcement's use of kid gloves on crowds who stormed the Capitol and the deployment of tear gas, excessive force, and helicopter overflights on social justice demonstrators this summer certainly justifies the outrage it has prompted. The solution, however, is not to insist that Trump supporters be subject to the same heavy-handed response. Rather, it is to insist that law enforcement strike the admittedly difficult balance between permitting valid acts of protest and preventing violence and destruction of property. It does not seem too much to ask that law enforcement protect law-abiding Trump supporters' right to express their views—note that armed protesters might not meet that description, given Washington D.C.'s strict firearms regulations—while simultaneously denying those supporters access to the floor of the Senate or House Speaker Nancy Pelosi's office. Just as it seems reasonable to allow protestors to take to the streets without having to fear being swept up in unmarked vehicles by individuals purporting to be law enforcement but refusing to identify themselves.

It is no wonder that Americans have responded to the events of Jan. 6 with rage, shock, and profound sadness. American democracy is currently in a state of seeming fragility that demands nurturing rather than the assault to which it was subject that day. The desecration of what many have described as the temple of that democracy should not go unanswered. That answer must not, however, further weaken the foundations of that temple by undermining the most American of rights: the right to engage in peaceful protest against our government.

* *Emily Berman is an Associate Professor at University of Houston Law Center.* *An earlier version of this piece appeared at Just Security on January 12, 2021.*

ARTICLE: Biological Threats Are National Security Risks: Why COVID-19 Should Be a Wake-up Call for Policy Makers

January 5, 2020

Reporter
77 Wash. & Lee L. Rev. Online 217 *

Length: 23740 words

Author: Representative Eric M. Swalwell * and R. Kyle Alagood **

* Member, United States House of Representatives (D-CA); B.A. University of Maryland, 2003; J.D., University of Maryland, 2006; Congressman Swalwell serves as Chair of the Subcommittee on Intelligence Modernization and Readiness of the House Permanent Select Committee on Intelligence.

** B.A. Louisiana State University, 2007; M.Sc. University College London, 2009; J.D. Louisiana State University Law Center, 2015.

Text

[*218] *I. Introduction*

COVID-19 demonstrates that a naturally occurring, communicable disease can threaten U.S. national security with deadly consequences. Upwards of 227,000 lives were lost in the United States due to COVID-19 between March and October 2020. Another 8.8 million people in the United States contracted the disease during the same time span. Those numbers continue to grow. [1]At the start of the pandemic, hospitals ran out of personal protective equipment for health care workers and life-saving ventilators for patients. The USS *Theodore Roosevelt* was almost entirely evacuated because sailors contracted the disease. Supply chains from toilet paper to pork were disrupted. For months, the nation's attention and resources were consumed by the disease. The U.S. president was hospitalized for three days due to COVID-19. And the country's highest-ranking military officers, the Joint Chiefs of Staff, were quarantined for two weeks in October after being exposed. COVID-19 revealed weaknesses in U.S. national security strategy, and the executive branch's response compounded the risks.

A national security strategy is the "nation's plan for the coordinated use of all the instruments of state power -- nonmilitary as well as military--to pursue objectives that defend and advance its national interest." [2]Perhaps the most straightforward national security objective is to protect the country from foreign invasion, but national security involves other objectives that aim to protect people in the United States as well as their values. For example,

---

1 *Covid in the U.S.: Latest Map and Case Count*, N.Y. TIMES, https://perma.cc/J9RU-HTCX (last updated Nov. 23, 2020, 12:46 PM).

2 Terry L. Deibel, *Strategy, National Security, in* 5 INTERNATIONAL MILITARY AND DEFENSE ENCYCLOPEDIA 2577, 2577-78 (Trevor N. Dupuy et al. eds., 1993).

protecting U.S. elections from foreign interference is a security objective that advances the nation's interest in democratic governance. The outbreak of a highly contagious disease like COVID-19 strikes at the core of national security and the nation's interest in protecting its citizens from unnecessary harm.

National security experts have warned that infectious diseases could result in human suffering, economic losses, and **[*219]** political instability. [3]They have explained that a pandemic or large-scale bioterrorist attack could cause mass casualties, overwhelm the health care system, quickly deplete medical supplies needed for treatment and to protect health care workers, [4]drain the workforce, and interrupt supply chains, [5]leaving the United States susceptible to other security risks while resources are focused on mitigating the biological threat. COVID-19 affirmed their warnings.

This article begins with an overview of U.S. national security strategy: what it is and why it is necessary. Part II describes the *National Security Strategy of the United States* and the *National Biodefense Strategy*: what they do and how they should work together. In Part III, the article compares and contrasts two presidents' development and execution of strategies in response to national security crises: how President John F. Kennedy's handling of the Cuban Missile Crisis and President Donald J. Trump's response to the COVID-19 pandemic differed. Part IV explores the COVID-19 pandemic's immediate and long-term effects on U.S. national security. And Part V suggests ways to ensure policy makers are prepared to combat biological threats in the future.

II. Understanding National Security Strategy

Defense and national security strategy have existed throughout history, but rapid scientific and technological development during the twentieth century fundamentally **[*220]** shifted security dynamics. In the past, national security strategy primarily focused on military threats abroad. Today, it broadly encompasses domestic and international threats, whether of a military or nonmilitary nature, including the threats posed by a naturally occurring communicable disease. Despite these advances, the core question for national security strategy now is fundamentally the same as it was centuries ago: how does a nation best utilize its resources to achieve desired security objectives? [6]

When the United States emerged from World War II as the global power, its military, intelligence, and foreign affairs capabilities were spread across numerous executive branch agencies. President Harry S. Truman and Congress recognized the need for a coordinated national security apparatus to ensure the United States could effectively respond to threats at home and around the world. After more than a year of negotiation with the Truman administration and military leaders, Congress passed the National Security Act of 1947 [7]to centralize the federal government's national security divisions and ensure the United States would have comprehensive, integrated policies for the

---

[3] *See* HEALTH & MED. DIV., NAT'L ACADS. OF SCI., ENG'G & MED., GLOBAL HEALTH AND THE FUTURE ROLE OF THE UNITED STATES 59 (2017), https://perma.cc/T8U4-8V4V (PDF) ("Infectious disease outbreaks clearly impose terrible costs in terms of human suffering and mortality, as well as economic costs that threaten progress and stability in countries around the world, and that greatly exceed the costs of prevention and preparedness measures . . . ." (citations omitted)). See also *Milley: COVID-19 Will Have Lasting Impact on Military*, ASS'N U.S. ARMY (Apr. 16, 2020), https://perma.cc/5U96-YM8K [hereinafter ASS'N U.S. ARMY], for a U.S. military leader's description of how COVID-19 could affect economic and political stability.

[4] *See* Roger Roffey et al., *Biological Weapons and Bioterrorism Preparedness: Importance of Public-Health Awareness and International Cooperation*, 8 CLINICAL MICROBIOLOGY & INFECTION 522, 525 (2002), https://perma.cc/4HGV-XQLJ (PDF) (noting the effect on the health care system of a bioweapon outbreak).

[5] HEALTH & MED. DIV., *supra* note 3, at 53-55.

[6] *See* DENNIS M. DREW & DONALD M. SNOW, MAKING TWENTY-FIRST-CENTURY STRATEGY: AN INTRODUCTION TO MODERN NATIONAL SECURITY PROCESSES & PROBLEMS 3-4 (2006), https://perma.cc/4Z4Z-SHSL (PDF) (describing the fundamentals of national security strategy in the modern military context).

[7] Ch. 343, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended at 50 U.S.C. §§ 3001-3238).

protection of its people. [8]Through the National Security Act, Congress reorganized the executive branch's military, intelligence, and foreign affairs operations; created the Central Intelligence Agency (CIA); and established the National Security Council. Over time, Congress has amended the National Security Act to reflect evolving threats and compel presidents to annually submit to Congress a comprehensive set of goals, objectives, and tactics for securing the country's interests at home and abroad. [9]

[*221] The National Security Act did not spring forth fully formed from the head of a god, like Athena. It was born out of the United States' new role as world leader during an era defined by rapid scientific and technological change. That law and its progeny recognize that national security strategy is no longer synonymous with military strategy and foreign affairs. Threats are increasingly technological, complex, or diffuse, which magnifies the roles of data collection, subject matter expertise, and information sharing. The federal government needs the best-available data--including, in some instances, covert intelligence--in order to analyze and respond to potential threats. People with subject matter expertise must analyze the data to assess potential threats. And government officials must work together to develop a comprehensive national security strategy that lays out how the nation can efficiently utilize its resources to achieve desired outcomes in light of data and threat assessments.

As new threats emerged during and after World War II, the evolution of the United States' national security strategy, formalized under the National Security Act, explains how a naturally occurring novel virus like COVID-19 fits under the expanding umbrella of security strategy. Technological advancements emerging from the Industrial Revolution allowed countries to develop long-range weapons such as military aircraft, the atomic bomb, ballistic missiles, unmanned aerial vehicles, and other innovations that shattered the illusion of invulnerability of the United States' domestic facilities, which had been sheltered from conflict by two oceans. [10]Scientific progression in the field of microbiology led countries to explore the weaponization of biological agents--bacteria, viruses, and fungi in particular--and to develop countermeasures for a biological attack. [11]And environmental degradation, easy travel among countries, and climate change increase the likelihood that naturally occurring pathogens will quickly spread around the world, making countries more susceptible to other security **[*222]** threats as they focus resources on combatting disease outbreaks. [12]

III. Developing the National Security Strategy of the United States and National Biodefense Strategy

In 1986, Congress modified the National Security Act to require that the U.S. president issue a yearly report laying out the national security strategy of the United States. [13]Although no president since Ronald Reagan has issued a yearly report, each president has produced at least one *National Security Strategy of the United States* (*NSS*) during each term in office. [14] *NSS* reports reflect national and global realities, but they historically center on occurrences in nation-states. For example, the 1991 *NSS* came on the heels of the Gulf War, collapse of the Soviet Union, and a U.S. economic recession, so it focused on diplomatic cooperation among countries, democracy

---

[8] *See* Charles A. Stevenson, *The Story Behind the National Security Act of 1947*, MIL. REV., May--June 2008, at 13, 13 (overviewing negotiations relating to the National Security Act).

[9] *See, e.g.*, Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433, 100 Stat. 992 (codified as amended in scattered sections of 10 U.S.C.).

[10] DREW & SNOW, *supra* note 6, at 6-10; Roger Roffey et al., *Biological Warfare in a Historical Perspective*, 8 CLINICAL MICROBIOLOGY & INFECTION 450, 450 (2002), https://perma.cc/VJ94-3ZTP (PDF).

[11] Roffey et al., *supra* note 4, at 523; Friedrich Frischknecht, *The History of Biological Warfare*, 4 EMBO REP. S47, S48 (2003), https://perma.cc/A9GU-UGTM (PDF).

[12] *See* Jim Robbins, *The Ecology of Disease*, N.Y. TIMES (July 14, 2012), https://perma.cc/C62A-FGPD (explaining the relationship between the environment and disease); JOSHUA W. BUSBY, CLIMATE CHANGE AND NATIONAL SECURITY 5-6 (2007), https://perma.cc/W5TY-4AAP (PDF) (describing the effects of climate change on national security).

[13] 50 U.S.C. § 3043.

[14] CATHERINE DALE, CONG. RSCH. SERV., R43174, NATIONAL SECURITY STRATEGY: MANDATES, EXECUTION TO DATE, AND ISSUES FOR CONGRESS 3 (2013), https://perma.cc/XE5T-U9Z7 (PDF).

building in former Soviet states, and economic security at home. [15]Then, following the 9/11 attacks, the United States shifted its focus from nation-states to non-state actors.

The 1990 *NSS* and successive reports had mentioned the national security threat posed by foreign nations' possession of biological weapons, but the threat posed by disease outside the military context was unmentioned until 1993. *NSS* reports from 1993 to 1997 treated disease predominantly as a threat to economic health. The 1999 *NSS* was the first to explain that an overseas outbreak of a naturally occurring disease could have "important implications for American security." [16]Then, in 2001, **[*223]** a series of anthrax attacks targeted national media and Congress, reshaping the threat dynamic to reflect the domestic threat posed by biological agents. During the month following the 9/11 terror attacks, an individual mailed letters containing anthrax to news outlets and two U.S. senators. The anthrax attacks killed five people and infected twenty-two others, sparking changes to federal law and prompting the George W. Bush administration to issue a directive laying out a national security strategy for future biothreats. [17]President Barack Obama's administration expanded and built upon the Bush directive, emphasizing the need to protect global health security and track the emergence of communicable disease, whether naturally occurring or bioengineered. [18]

In 2015, a panel of national security experts convened the Blue Ribbon Study Panel on Biodefense, which found that "[t]he United States is underprepared for biological threats. Nation states and unaffiliated terrorists (via biological terrorism) and nature itself (via emerging and reemerging infectious diseases) threaten us." [19]The Blue Ribbon Study Panel found that the United States had no comprehensive national strategy for responding to biological threats, and responsibility was spread across more than a dozen federal agencies or departments, with more than four dozen federal officials in charge of biopreparedness. [20]The Blue Ribbon Study Panel's findings **[*224]** spurred Congress to include a provision in the National Defense Authorization Act for Fiscal Year 2017 requiring the secretaries of Defense, Health and Human Services, Homeland Security, and Agriculture to develop a comprehensive national biodefense strategy. [21]

The Trump administration issued both an updated *NSS* and a *National Biodefense Strategy* (*NBS*). The *NSS* explicitly addresses natural disease outbreaks such as COVID-19:

> Biological threats to the U.S. homeland--whether as the result of deliberate attack, accident, or a natural outbreak--are growing and require actions to address them at their source . . . . At home, we will strengthen our emergency response and unified coordination systems to rapidly characterize outbreaks, implement public health

---

[15] *See generally* WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES (1991), https://perma.cc/BY63-LNF5 (PDF).

[16] *See* WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY 1 (1999), https://perma.cc/URV5-M85D (PDF) ("Other problems originating overseas--such as resource depletion, rapid population growth, environmental damage, *new infectious diseases*, pervasive corruption, and uncontrolled refugee migration--have increasingly important implications for American security." (emphasis added)).

[17] Rachel Long, *Bioterrorism in the 21st Century*, GLOB. AFFS. REV. (Apr. 11, 2018), https://perma.cc/A6KG-3HMR.

[18] Gregory D. Koblentz, *From Biodefense to Biosecurity: The Obama Administration's Strategy for Countering Biological Threats*, 88 INT'L AFF. 131, 131-33 (2012), https://perma.cc/U3FN-3XFV (PDF).

[19] Joseph I. Lieberman & Thomas J. Ridge, *Preface* to BLUE RIBBON STUDY PANEL ON BIODEFENSE, BIPARTISAN COMM'N ON BIODEFENSE, A NATIONAL BLUEPRINT FOR BIODEFENSE: LEADERSHIP AND MAJOR REFORM NEEDED TO OPTIMIZE EFFORTS, at iv (2015), https://perma.cc/6LSB-6HST (PDF).

[20] *Id.*; Rachel Bartholomew & Kristin Omberg, *Making Sense of the 2018 National Biodefense Strategy*, BULL. ATOMIC SCIENTISTS (Jan. 18, 2019), https://perma.cc/F6A7-X8FM ("[T]he 2015 bipartisan report of the Blue Ribbon Study Panel on Biodefense warned that despite 'a decade of profusion of policy directives,' the United States had failed to produce a *comprehensive* biodefense strategy spanning prevention to recovery." (emphasis added)).

[21] *Id.*; National Defense Reauthorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2000.

containment measures to limit the spread of disease, and provide surge medical care--including life-saving treatments. [22]

The *NBS* extends beyond a purely governmental approach to protecting against a biological threat. It lays out a plan for the federal government to work alongside state, local, tribal, medical, and industry leaders to prevent and mitigate biological risks. [23]It makes key assumptions about biological threats, whether naturally occurring, including that "[b]iological [t]hreats are [p]ersistent," "[o]riginate from [m]ultiple [s]ources," and "[d]o [n]ot [r]espect [b]orders." [24]Among other prescriptions for responding to biological threats, the *NBS* calls for the federal government to "[d]evelop, exercise, and update prevention, response, and recovery plans and capabilities"; "[e]stablish capability to provide surge staffing, resources, and supplies" to state, local, and tribal governments' public health departments; coordinate with all levels of government to develop clinical guidance for triage and management of disease outbreaks; conduct pre-incident planning for the distribution of federal medical countermeasures stockpiles, including personal **[*225]** protective equipment; and "provide clear, consistent, and coordinated information" to the public. [25]

IV. Executing the Strategy

National security strategies can be effective only if decision makers have clear objectives and are capable of listening to diverse perspectives, digesting information, revising courses of action based on new data, and following through with the strategic plan. In contrast, a decision maker who distrusts experts, rejects intelligence, acts according to gut instincts, and rejects strategy can endanger national security. President John F. Kennedy's handling of the Cuban Missile Crisis in 1962 is a case study in effective national security leadership. President Donald J. Trump's response to COVID-19 illustrates how a capricious and disinterested decision maker can derail evidence-based strategy and endanger national security.

A. The Cuban Missile Crisis

Throughout 1962, the Soviet Union had increased its military presence in Cuba, leading President John F. Kennedy to issue a statement on September 4, laying out the United States' national security objective vis-à-vis Cuba's growing military relationship with the Soviet Union: "It continues to be the policy of the [U.S.] that the Castro regime will not be allowed to export its aggressive purposes by force or the threat of force. It will be prevented by whatever means may be necessary from taking action against any part of the Western Hemisphere." [26]To put it succinctly, it was the policy of the United States that Cuba not acquire offensive or nuclear weapons capabilities. A month later, however, the world was on the brink of nuclear war, and the post-World War II national security reorganization passed by Congress would be put to the test.

On October 14, 1962, a U.S. Air Force reconnaissance flight captured photographs of what appeared to be Soviet nuclear **[*226]** missile installations in Cuba, which would mean Cuba had access to offensive weapons in violation of Kennedy's policy to keep such weapons out of the Castro regime's hands. Before sounding the alarm, military intelligence verified the images, then consulted with the CIA to ensure the data and analysis from the photographs were accurate. After verifying what the photographs showed, the CIA shared the information with National Security

---

[22] WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 9 (2017), https://perma.cc/2VZ2-3ZK4 (PDF).

[23] WHITE HOUSE, NATIONAL BIODEFENSE STRATEGY, at i (2018), https://perma.cc/47X2-GFJD (PDF).

[24] *Id.* at 3-4.

[25] *Id.* at 16-18.

[26] John F. Kennedy, President, U.S. Reaffirms Policy on Prevention of Aggressive Actions by Cuba, Statement Read to News Correspondents by Pierre Salinger, the White House Press Secretary (Sept. 4, 1962), *in* DEP'T ST. BULL., Sept. 1962, at 450.

Advisor McGeorge Bundy. Bundy then presented the data and expert analysis to Kennedy. [27]The centralized and coordinated national security apparatus envisioned by Congress in the National Security Act of 1947 had worked. The military and CIA had worked together to gather and analyze data, then passed it along to the White House through the National Security Advisor. It was up to Kennedy to develop and execute a strategy that would achieve the United States' objective to keep offensive weapons out of Cuba.

Upon receiving a briefing from Bundy, Kennedy immediately assembled a group of advisers with expertise in national security, foreign affairs, and domestic affairs to assess the United States' resources and craft strategies to remove the missiles from Cuba. That group, known as ExComm (short for Executive Committee of the National Security Council), was comprised of cabinet members, military brass, diplomats, and intelligence officials, as well as trusted advisers who understood the potential political fallout in the United States. ExComm was tasked with reviewing data, including ongoing surveillance, and developing options for dealing with the missile threat. During ExComm meetings, Kennedy took charge. He engaged with maps, intelligence, and military tactics; challenged his advisers' ideas and pushed them to think through geopolitical repercussions of potential U.S. actions; and never stopped asking questions. [28]

ExComm presented Kennedy with three main responses to remove the missiles from Cuba: Military action, diplomacy, or a blockade. Military action included air strikes against the missile **[*227]** sites, wider air strikes against the missile sites and military targets, invasion, or some combination thereof. Diplomatic efforts centered on offering to remove U.S. nuclear missiles from Turkey in exchange for the removal of Soviet nuclear missiles in Cuba. And a blockade would involve either preventing arms from reaching Cuba or cutting off all supplies from reaching the island. [29]On October 24, before settling on a course of action, Kennedy consulted with congressional leaders representing both parties in the House and Senate to get their input on responding to the crisis. Like many ExComm members including all Joint Chiefs of Staff, congressional leaders favored strong military intervention and thought a blockade would be the weakest response. [30]

Throughout the crisis, Kennedy was reticent about military intervention, and a blockade under international law would presume the existence of armed conflict. After days of deliberating with experts and consulting with Congress, Kennedy settled on a strategic plan to get the missiles out of Cuba. He would publicly announce a blockade (euphemistically referred to as a "quarantine" to avoid the international law implications) to prevent Soviet weapons from entering Cuba and privately enter into a diplomatic deal to remove U.S. Jupiter missiles from Turkey in exchange for the removal of Soviet missiles from Cuba. Congress and the public would know about the quarantine, but the diplomatic exchange would remain secret to all but a few individuals inside the Kennedy administration. Kennedy followed through with his two-pronged plan, despite pressure from military leaders and high-ranking members of Congress to pursue a more aggressive strategy. His strategy worked. The Soviet Union withdrew its missiles from Cuba, the United States later withdrew its missiles from Turkey, and the immediate threat of nuclear war dissipated.

[*228] *B. The COVID-19 Pandemic*

President Donald J. Trump's response to COVID-19, the global pandemic that shut down much of the United States for most of 2020, demonstrates how national security threats can cripple the country if left unmitigated. On December 31, 2019, Wuhan Municipal Health Center in China reported a cluster outbreak of pneumonia with an unknown cause. During the first week of January 2020, the cause was identified as a novel coronavirus, which was labeled SARS-CoV-2. Shortly after SARS-CoV-2 was identified, the disease it caused, referred to as COVID-19, spread to Thailand, Japan, South Korea, Europe, and the United States. On January 20, the first identified case of COVID-19 appeared

---

[27] THE CUBAN MISSILE CRISIS, 1962: A NATIONAL SECURITY ARCHIVE DOCUMENTS READER 358-59 (Laurence Chang & Peter Kornbluh eds., 1992).

[28] *See* McGeorge Bundy & James G. Blight, *October 27, 1962: Transcripts of the Meetings of the ExComm*, 12 INT'L SEC. 30 (1987), https://perma.cc/XUD6-Q85Y (PDF) (transcribing and annotating presidential recordings of ExComm meetings).

[29] *Id.*

[30] 2 THE PRESIDENTIAL RECORDINGS: JOHN F. KENNEDY 52-81 (Timothy Naftali & Philip Zelikow eds., 2001).

in the United States, and on January 30, the U.S. Centers for Disease Control and Prevention (CDC) reported the first case of human-to-human transmission of COVID-19 in the country. [31]

The Trump administration was not without a plan for dealing with a national-security threat in the form of a contagious disease. It was without leadership. Despite his own administration having released a *National Biodefense Strategy*, Trump's plan for COVID-19 was to "Just stay calm. It will go away." [32]The *NBS* called for the federal government to develop, practice, and revise a biothreat response plan, but a year and a half before COVID-19 began spreading around the world, the Trump administration dismantled the National Security Council's pandemic response team. [33]Trump would not appoint a centralized COVID-19 response team until the disease had infected at least sixty people in the United States. And unlike Kennedy, who took an active leadership role in ExComm **[*229]** meetings, Trump only sporadically attended meetings of the response team. [34]

The *NBS* called for the federal government to plan in advance for the distribution of federal medical countermeasures stockpiles, including personal protective equipment, and to provide resources and supplies to state, local, and tribal governments, but the Strategic National Stockpile ran out of N-95 respirators and other medical equipment direly needed by health care providers during the COVID-19 pandemic. A senior advisor to Trump contradicted the *NBS* and said that the stockpile was "not supposed to be states' stockpiles that they then use," then the Trump administration revised the Strategic National Stockpile's website to downplay the federal government's role regarding the provision of resources and supplies to states during a disease outbreak. [35]And the *NBS* emphasized the need for clear, consistent, and coordinated information from the federal government during a biological event, a strategy President Trump ignored as he openly contradicted his own experts' assessments and publicly floated unscientific (and sometimes life-threatening) ideas for treating COVID-19. [36]

Throughout his tenure in office, Trump had attacked the intelligence community, going as far as describing his own intelligence officials as "passive and naive" and telling them to "go back to school" while they testified in Congress about threats emanating from Iran. [37]Trump's distrust of the intelligence community helps explain, in part, his slow response to COVID-19. Whereas Kennedy relied heavily on data and **[*230]** intelligence to inform his plans to mitigate the Cuban Missile Crisis, Trump ignored warnings from intelligence officials, epidemiologists, and global health experts about COVID-19. By mid-January 2020, U.S. national security intelligence was clear that COVID-19 was a pandemic risk that could reach the United States. According to *Washington Post* reporting, COVID-19 comprised a majority of the intelligence data in the President's Daily Brief, [38]which is a daily summary of the most pressing high-level intelligence produced for and presented to the president. Intelligence reports presented to

---

[31] *A Timeline of COVID-19 Developments in 2020*, AM. J. MANAGED CARE (July 3, 2020), https://perma.cc/7EFW-L9TK.

[32] President Donald J. Trump, *Remarks by President Trump After Meeting with Republican Senators*, WHITE HOUSE (Mar. 10, 2020, 1:57 PM), https://perma.cc/2LFU-ZELB.

[33] Deb Reichmann, *Trump Disbanded NSC Pandemic Unit That Experts Had Praised*, U.S. NEWS & WORLD REP. (Mar. 14, 2020), https://perma.cc/QX79-UHHX.

[34] Ashley Parker, Yasmeen Abutaleb & Josh Dawsey, *Trump Administration Has Many Task Forces--But Still No Plan for Beating COVID-19*, WASH. POST (Apr. 11, 2020, 8:45 PM), https://perma.cc/9EQPK47G.

[35] Adam Clark Estes, *America's Emergency Medical Stockpile is Almost Empty. Nobody Knows What Happens Next.*, VOX, https://perma.cc/DXH9-KTCR (last updated Apr. 7, 2020, 11:20 AM).

[36] *See* Libby Cathey, *Trump Versus the Doctors: When the President and His Experts Contradict Each Other*, ABC NEWS (Apr. 24, 2020, 6:55PM), https://perma.cc/S6VW-W2H3.

[37] Donald J. Trump (@realdonaldtrump), TWITTER (Jan. 30, 2019, 7:50 AM), https://twitter.com/realdonaldtrump/status/1090608298343190528; Donald J. Trump (@realdonaldtrump), TWITTER (Jan. 30, 2019, 7:56 AM), https://twitter.com/realdonaldtrump/status/1090609577006112769.

[38] Greg Miller & Ellen Nakashima, *President's Intelligence Briefing Book Repeatedly Cited Virus Threat*, WASH. POST (Apr. 27, 2020, 4:22 PM), https://perma.cc/3WRU-HJMA.

the president became an "insistent drumbeat" warning about the danger of COVID-19 in the United States, according to administration officials. [39]In a February 7 phone call with journalist Bob Woodward, Trump privately said that COVID-19 "goes through air. . . . You just breathe the air and that's how it's passed. . . . It's also more deadly than your strenuous flus. . . . This is deadly stuff." [40]In public, Trump downplayed the risk. On February 19, he proclaimed, "I think it's going to work out fine. I think when we get into April, in the warmer weather, that has a very negative effect on [COVID-19]." [41]Without evidence, he told the country, "the Coronavirus is very much under control in the USA." [42]On February 26, he stated, again without evidence, that "within a couple of days[,COVID-19] is going to be down to close to zero." [43]During a *Fox News* interview on March 4, Trump called COVID-19 the **[*231]** "corona flu" then implied that COVID-19 was less lethal than influenza. [44]Unlike Kennedy, who digested intelligence reports on the Soviet threat in Cuba and took the matter seriously, Trump appears not to have trusted the intelligence and data on COVID-19, which delayed the federal response to the disease and foreclosed the possibility of containment.

It is not just Trump's distrust of data and delayed action on COVID-19 that contrasts with Kennedy's response to Soviet missiles in Cuba. Kennedy actively engaged with data and respected the role of experts, even those who did not agree with him. He assembled an expert advisory group within hours of receiving intelligence assessments about the Soviet missiles in Cuba. He included the Joint Chiefs of Staff in that group, even though Kennedy distrusted them after the failed Bay of Pigs invasion. Trump and his administration, on the other hand, showed disdain for expertise. Only after COVID-19 had begun to spread in the United States did Trump begin to take the disease seriously and appoint a task force on COVID-19. The task force was comprised of preeminent infectious disease experts including Dr. Anthony Fauci, head of the National Institute of Allergy and Infectious Diseases; Dr. Deborah Birx, who is a leading expert on HIV/AIDS and global health; Surgeon General Jerome Adams; and other administration officials; but Trump publicly contradicted his own experts' assessments when they did not fit with his worldview. For example, at an April 21 briefing, CDC Director Dr. Robert Redfield warned that a second wave of COVID-19 could be deadlier than the first wave, then Trump claimed the opposite: "[W]e will not go through what we went through for the last two months . . . It might not come back at all." [45]Dr. Fauci had to correct the president, saying, "We will have coronavirus in the fall. I am convinced of that because of the degree of transmissibility that it has, the global nature." [46]Perhaps most tellingly, Trump, who is not a doctor, began promoting the untested, off-label use of a prescription drug called hydroxychloroquine to treat COVID-19, **[*232]** despite experts' warnings that the drug could have dangerous complications and had not been shown to affect COVID-19. [47]

---

[39] *Id.*

[40] Robert Costa & Philip Rucker, *Woodward Book: Trump Says He Knew Coronavirus was 'Deadly' and Worse Than the Flu While Intentionally Misleading Americans*, WASH. POST (Sept. 9, 2020, 10:55 AM), https://perma.cc/QGD2-YBL6 (interview with President Donald J. Trump available in audio player captioned, "Listen: In a Feb. 7 interview, when asked what Chinese President Xi Jinping told him about the virus, Trump says, 'This is deadly stuff.'").

[41] Interview by Kari Lake, Fox 10 Phoenix, with President Donald J. Trump (Feb. 19, 2020), https://perma.cc/XU4Y-TFBK.

[42] Donald J. Trump (@realdonaldtrump), TWITTER (Feb. 24, 2020, 3:42 PM), https://twitter.com/realdonaldtrump/status/1232058127740174339.

[43] Jonathan Chait, *Trump: I Was Right, Coronavirus Cases 'Will Go Down to Zero, Ultimately'*, N.Y. MAG. INTELLIGENCER (Apr. 28, 2020), https://perma.cc/R8YY-BGBE.

[44] Aaron Rupar, *"This Is Just My Hunch": Trump Goes on Fox News and Spreads Misinformation About the Coronavirus*, VOX (Mar. 5, 2020, 10:45 AM), https://perma.cc/3U8V-NNFV.

[45] Cathey, *supra* note 36.

[46] *Id.*

[47] Jordan Culver & Rebecca Morin, *'He's Answered That Question.' Trump Interrupts When Reporter Asks Fauci About Hydroxychloroquine*, USA TODAY (Apr. 6, 2020, 11:23 AM), https://perma.cc/3USR-QFD6. On May 18, 2020, Trump announced that he was taking hydroxychloroquine as a prophylactic, despite the Food and Drug Administration having warned against the use of hydroxychloroquine for COVID-19 treatment outside a hospital setting due to the drug increasing a person's risk of heart

Starting in March, while Trump was still downplaying the virus's risk, states began issuing shelter-in-place orders, shutting down non-essential businesses, travel, and gatherings to slow the spread of COVID-19. On April 19, after the United States had been at a standstill for more than a month, Trump, in consultation with the task force and public health officials, released a strategy to safely reopen the country in phases as states meet certain criteria with regard to COVID-19 cases. The strategy's first phase would allow for states to begin opening certain sectors, excluding schools and other areas where social distancing is difficult, provided that a state had seen a decline of documented COVID-19 cases over a two-week period or a decline in positive tests as a percent of total COVID-19 tests over a two-week period. [48]A week later, Trump seemed to abandon his own reopening strategy and the advice of public health experts, telling governors to "start thinking about school openings." [49]By May, he had entirely abandoned his own strategy and was commending states for reopening even though **[*233]** they had not met the phase-one criteria, [50]a move Dr. Fauci said may cause "suffering and death that could be avoided." [51]In the seven months following Dr. Fauci's warning, COVID-19 cases spiked, killing more than 180,000 Americans. [52]

V. Immediate and Long-Term Effects of COVID-19 on National Security

COVID-19's effects on U.S. national security evolved as the country sporadically emerged from months of social distancing and local shelter-in-place orders; however, it is clear that the pandemic harmed military readiness, laid bare to all that the United States is susceptible to biological threats, and helped cultivate violent extremism.

A. Immediate Effects on Military Readiness and Security

The nature of military readiness requires large groups of service members to live, train, and work together in proximity. Starting in March 2020, the U.S. military reported that between 100 and 200 service members each day were testing positive for COVID-19. [53]By late May, the U.S. Department of Defense reported 6,168 cumulative cases of COVID-19 in the military, with more than 3,000 additional cases among military dependents, contractors, and civilian workers. [54]The cumulative number of Department of Defense COVID-19 cases in early October

---

problems. Trump suffers from heart disease. In October, he contracted COVID-19 and was hospitalized. Annie Karni & Katie Thomas, *Trump Says He's Taking Hydroxychloroquine, Prompting Warning from Health Experts*, N.Y. TIMES (May 18, 2020), https://perma.cc/6C3C-BZ6E; Sanjay Gupta, *President Trump Has Common Form of Heart Disease*, CNN (Feb. 1, 2018, 3:03 PM), https://perma.cc/W5C5-S26G; Kevin Liptak, *Trump Taken to Walter Reed Medical Center and Will Be Hospitalized 'For the Next Few Days'*, CNN (Oct. 3, 2020, 1:19 AM), https://perma.cc/FYB8-EVPV.

[48] WHITE HOUSE & CTRS. FOR DISEASE CONTROL & PREVENTION, GUIDELINES FOR OPENING UP AMERICA AGAIN (2020), https://perma.cc/P4H7-KQG3 (PDF).

[49] Katherine Faulders & Ben Gittleson, *Trump Encourages Governors to 'Seriously Consider' Reopening Schools*, ABC NEWS (Apr. 27, 2020, 3:25 PM), https://perma.cc/P6SF-JJVU.

[50] Toluse Olorunnipa, Griff Witte & Lenny Bernstein, *Trump Cheers on Governors Even as They Ignore White House Coronavirus Guidelines in Race to Reopen*, WASH. POST (May 4, 2020, 9:10 PM), https://perma.cc/9RY8-UFGW.

[51] John Wagner et al., *Fauci Warns Senate That Reopening U.S. Too Quickly Could Lead to Avoidable 'Suffering and Death'*, WASH. POST (May 12, 2020, 2:36 PM), https://perma.cc/NMK5-R5X7.

[52] *Compare COVID-19 United States Cases by County*, JOHNS HOPKINS UNIV. (2020), https://perma.cc/7SC5-VLCT (totaling 259,900 deaths as of November 24, 2020), *with US Historical Data*, COVID TRACKING PROJECT, ATLANTIC, https://perma.cc/9HLH-WXR7 (last updated Dec. 21, 2020) (totaling 79,040 deaths as of May 12, 2020).

[53] Meghann Myers, *The Military Continues to Diagnose More Than 100 New COVID-19 Cases a Day*, MIL. TIMES (Apr. 20, 2020), https://perma.cc/T3BP-K53V.

[54] Jennifer-Leigh Oprihory, *Snapshot: DOD and COVID-19*, AIR FORCE MAG. (May 27, 2020), https://perma.cc/Z7XH-CCLM.

exceeded 47,500 military service members, 10,000 **[*234]** civilian workers, 6,000 military dependents, and 4,000 contractors, with nearly 100 deaths recorded. [55]

On March 24, the USS *Theodore Roosevelt* (*TR*) reported that three service members had contracted COVID-19. The Department of Defense evacuated those service members but did not remove other sailors or sanitize the ship. The *TR*'s captain, Brett Crozier, sent a letter to his superiors and other Navy officials, complaining that the Navy was not adequately responding to the threat COVID-19 posed for sailors. Crozier wrote that the *TR* was unable to implement social-distancing guidelines recommended by the CDC and U.S. Navy, and urged evacuation of all service members except a small crew to maintain the ship's reactor. In his letter, Crozier said, "Decisive action is required now in order to comply with CDC and [Navy] guidance and prevent tragic outcomes." [56]Following the letter, the Navy began evacuating sailors from the *TR* to quarantine in Guam, then relieved the captain of duty, ostensibly for exercising poor judgment. [57]By April 3, the aircraft carrier had reported more than 100 positive cases. [58]Nearly 1,200 sailors out of 4,865 onboard ultimately tested positive for COVID-19. [59]After two months of quarantine, the *TR* reentered service with precautions against COVID-19, including mandatory face masks, but thirteen sailors retested positive weeks later. [60]The *TR*'s struggle to contain and mitigate COVID-19 is a microcosm **[*235]** of how a communicable disease can damage military readiness on a larger scale.

COVID-19 did more than hamper immediate military readiness. Its disruptions may have long-lasting consequences for the nation's armed forces. The pandemic forced the military to postpone exercises that are critical for ensuring U.S. service members and allied forces can quickly respond to military threats. [61]Social-distancing measures, necessary for mitigating the spread of COVID-19, interrupted military recruitment, leading to a decrease in the number of people entering military training and creating a gap that is likely to cause the military to fall short of its end-strength goals. [62]At the same time, according to General Mark Milley, Chairman of the Joint Chiefs of Staff, "There's significant stress as a result of this COVID-19 virus on the internal politics in other countries, on their economies, on resources. There is an increased probability or at least a risk of instability, significant instability, in some countries," [63]which heightens the need for U.S. military forces to be at peak operational performance in a post-COVID-19 world.

---

[55] Jennifer-Leigh Oprihory, *Snapshot: DOD and COVID-19*, AIR FORCE MAG. (Oct. 7, 2020), https://perma.cc/JH3F-W4C3.

[56] Matthias Gafni & Joe Garofoli, *Exclusive: Captain of Aircraft Carrier with Growing Coronavirus Outbreak Pleads for Help from Navy*, S.F. CHRON. (Mar. 31, 2020), https://perma.cc/2JRN-VLQY (last updated June 8, 2020).

[57] Bradley Peniston & Kevin Baron, *Aircraft Carrier Captain Fired for 'Poor Judgement' in Sending Coronavirus Letter*, DEF. ONE (Apr. 2, 2020, 7:18 PM), https://perma.cc/7ZX9-5F7B.

[58] Lindsay Cohn, Alice Friend & Jim Golby, *This Is What Was So Unusual About the U.S. Navy Making Captain Brett Crozier Step Down*, WASH. POST (Apr. 5, 2020, 6:00 AM), https://perma.cc/PN69-PPVJ.

[59] Luis Martinez, *USS Theodore Roosevelt Captain Confident Ship Can Deal With New COVID-19 Cases*, ABC NEWS (May 23, 2020, 1:36 PM), https://perma.cc/5RTB-PYTJ.

[60] Sarah McCammon, *13 USS Roosevelt Sailors Test Positive for COVID-19, Again*, NPR (May 16, 2020, 11:46 AM), https://perma.cc/4XBH-83GE.

[61] *See* Ryan Browne & Zachary Cohen, *US Military Curtails Another Major Exercise Due to Coronavirus Pandemic*, CNN (Mar. 16, 2020, 1:29 PM), https://perma.cc/R95J-ENX2 (covering the curtailment of U.S. military exercises); Barbara Starr, *US-South Korea Military Exercises Expected to be Scaled Back Due to Coronavirus*, CNN (Feb. 25, 2020, 2:31 PM), https://perma.cc/TJ9H-3HH8 (describing the cancellation of US-South Korea joint exercises and effects on long-term security); *see also Exercises and Training*, SUPREME HEADQUARTERS ALLIED POWERS IN EUR., N. ATL. TREATY ORG., https://perma.cc/Z4UP-SLVB (explaining why joint military exercises are necessary).

[62] Jennifer Steinhauer, *No More 'Kneecap to Kneecap' Talks: Coronavirus Hinders Military Recruiting*, N.Y. TIMES (May 20, 2020), https://perma.cc/R93K-L4UV; Brian W. Everstine, *DOD's End Strength Takes Hit Because of Coronavirus*, AIR FORCE MAG. (Apr. 28, 2020), https://perma.cc/NHT9-86JM.

[63] ASS'N U.S. ARMY, *supra* note 3.

Above COVID-19's direct impact on military readiness, the pandemic showed the United States' susceptibility to a targeted biological attack, which likely would involve pathogens, perhaps bioengineered, that could be deadlier and more easily transmittable than COVID-19; and failure of governments, even in high-income nations, to contain the virus **[*236]** likely made biological attacks more attractive to terrorists. [64]At its height in the spring of 2020, COVID-19 overwhelmed hospitals in cities across the United States, which put lives at risk and made the nation susceptible to other threats as health care resources quickly dried up across the country. The Trump administration had allowed the National Strategic Stockpile to become so woefully depleted that the federal government initially distributed only 11.7 million N-95 respirators, which accounted for 90 percent of the nation's reserves--even though the Trump administration estimated the United States would need 3.5 billion masks. [65]Facing a critical shortage of ventilators needed to help patients with severe COVID-19 symptoms breathe, hospitals were forced to modify ventilators to serve more than one patient and consider do-not-resuscitate orders for some patients in order to ensure those most likely to recover had access to the life-saving devices. [66]And COVID-19 hotspots quickly ran short on health care professionals, which required tens of thousands of doctors and nurses from areas with low rates of COVID-19, even those trained in fields unrelated to the **[*237]** disease, to voluntarily travel to alleviate the shortage of medical staff in hard-hit areas. [67]

By March 31, the outbreak's epicenter had shifted from the West Coast to New York City, where COVID-19 cases numbered 38,000. Hospitals, overwhelmed with COVID-19 patients and resultant deaths, set up makeshift morgues in refrigerated trucks. Hospitals ran out of personal protective equipment, such as N-95 respirators and gowns, and ventilators. Health care professionals were left to improvise, wearing homemade cloth masks, using trash bags as gowns, and modifying ventilators to serve two patients at a time. [68]Within a few months of COVID-19 entering the United States, thousands of health care workers had contracted the disease, and hundreds of them died. [69]COVID-19 overwhelmed the country's health care system, resulting in deaths that might have been prevented had the executive branch followed its own national security and biodefense strategies, but the effects of a health care system stretched beyond its capacity did not end there. More than 259,000 lives in the United States were lost to

---

[64] *See* ANDREW SILKE, POOL RE SOLS., COVID-19 AND TERRORISM: ASSESSING THE SHORT- AND LONG-TERM IMPACTS 7 (2020), https://perma.cc/3K4X-87QW (PDF) ("One genuine concern is that COVID-19 may lead to a resurgence in interest among terrorists for using [Chemical, Biological, Radiological, and Nuclear] weapons."); Gary Ackerman & Hayley Peterson, *Terrorism and COVID-19: Actual and Potential Impacts*, 14 PERSPS. ON TERRORISM 59, 64 (2020), https://perma.cc/35QW-5EP2

> The inability of even highly developed countries to stop the spread of the virus and the often incoherent and delayed responses of authorities at all levels have exposed the myriad weaknesses present in global public health systems. Such outcomes will not go unnoticed by terrorist groups, who will remember these impacts when seeking new means to achieve their goals. It must be remembered that a key strategy of terrorism is to inflict psychological damage on populations as a means of coercion . . . . The societal disruption, economic damage, and deaths caused by COVID-19 are a perfect script for the theatre of terrorism.

[65] Press Release, Comm. on Oversight & Gov't Reform, House of Representatives, New Document Shows Inadequate Distribution of Personal Protective Equipment and Critical Medical Supplies to States (Apr. 8, 2020), https://perma.cc/7PNB-M3HD.

[66] *Amid Grave Shortage of Ventilators, Some Hospitals Start Sharing Between Patients, Searching for Alternatives*, KAISER HEALTH NEWS (Mar. 26, 2020), https://perma.cc/5DRM-HYMK.

[67] Christina Farr, *Doctors and Nurses Are Signing Up for the Coronavirus Fight in Hotspots Like New York, but Many Fear They'll Be Needed Back Home*, CNBC (Apr. 9, 2020, 4:07 PM), https://perma.cc/E7NEQRZR.

[68] Michael Rothfeld et al., *13 Deaths in a Day: An 'Apocalyptic' Coronavirus Surge at an N.Y.C. Hospital*, N.Y. TIMES (Mar. 25, 2020), https://perma.cc/KXX8-CSR7 (last updated Apr. 14, 2020).

[69] Will Stone & Carrie Feibel, *COVID-19 Has Killed Close to 300 Health Care Workers, New Data from CDC Shows*, NPR (May 28, 2020, 6:00 AM), https://perma.cc/GR25-HUDG.

COVID-19 in just eight months, [70]demonstrating to bad actors that a biological event could efficiently cause deaths on a scale greater than the detonation of a 150 kiloton W-80 thermonuclear warhead in San Francisco. [71]

[*238] *B. Long-Term Effects on Race-Based and Anti-Government Violence*

The long-term effects of COVID-19 on national security will not be known until long after the pandemic has ended, but the disease itself and the Trump administration's bungled response have made the United States more susceptible to violent extremism.

As COVID-19 spread across the globe, governments sought to contain the deadly virus by restricting public gatherings and social interaction. Many countries, including the United States, shut down all but the most essential businesses and limited public interactions. [72]Much of the retail, food, and drink industries in the United States, which employ 26 million people, shuttered almost overnight. [73]Schools closed. Courts went online. COVID-19 disrupted people's lives and destroyed their livelihoods. As discussed in Part IV.B. above, President Donald J. Trump refused to implement a national strategy for combatting the pandemic, leaving mayors and governors to apply a patchwork of public health policies, including business closures and stay-at-home orders, in their own jurisdictions. And the president sowed distrust in government by attacking public health experts, media, and other elected officials who criticized his inaction. Public confusion about COVID-19, their fear of an unknown disease, social isolation, and economic turmoil fueled anxiety and depression in the United States, which has increased as shutdowns continued [74]--conditions that "arguably make a greater number of people more susceptible to radicalizing narratives that seek to scapegoat various 'others' and promise simple solutions." [75]

[*239] Social media has been the tool for extremists to prey on people and promote violence. [76]American University Professor Cynthia Miller-Idriss described COVID-19 and the necessary public health shutdown measures as having presented a "perfect storm for extremist recruitment" because of the "vast and evolving ecosystem of toxic online spaces, combined with potentially unprecedented amounts of time online and increasing anxiety and isolation for some," especially young people. [77]According to the Institute for Strategic Dialogue, "COVID-19 has been seized by far-right groups as an opportunity to call for extreme violence. This includes mobilisation by white supremacist communities as well as the increased prevalence of memes which semi-ironically promote insurrectional violence across a range of social media platforms." [78]By disrupting people's routines and fostering anxiety on

---

[70] *See supra* note 52 and accompanying text.

[71] *See* NUKEMAP, NUCLEAR SECRECY BLOG, https://perma.cc/8MKYPFJM.NUKEMAP is an educational resource created by Alex Wallerstein, an Assistant Professor of Science and Technology Studies at Stevens Institute of Technology, for evocative modeling. *Frequently Asked Questions About the NUKEMAP*, NUCLEAR SECRECY BLOG, https://perma.cc/ZYD5-UDAH (last updated June 2019).

[72] Daniel Dunford et al., *Coronavirus: The World in Lockdown in Maps and Charts*, BBC (Apr. 6, 2020), https://perma.cc/NC3B-4LTJ.

[73] Rakesh Kochhar & Amanda Barroso, *Young Workers Likely to Be Hard Hit As COVID-19 Strikes a Blow to Restaurants and Other Service Sector Jobs*, PEW RSCH. CTR. (Mar. 27, 2020), https://perma.cc/GA3U-N3MC.

[74] Anita Raj et al., *Time from COVID-19 Shutdown, Gender-Based Violence Exposure, and Mental Health Outcomes Among a State Representative Sample of California Residents*, 26 ECLINICALMEDICINE, Sept. 2020, at 4-7, https://perma.cc/4CHG-RTAE (PDF).

[75] Ackerman & Peterson, *supra* note 64, at 61 (citations omitted).

[76] *See* INST. FOR STRATEGIC DIALOGUE, COVID-19 DISINFORMATION BRIEFING NO. 2: FAR-RIGHT MOBILISATION 1, 2 (2020), https://perma.cc/4XJUVCAR(PDF).

[77] Cynthia Miller-Idriss, Opinion, *We're Living in a Perfect Storm for Extremist Recruitment. Here's What We Can Do to Stop It*, CNN (July 19, 2020, 6:57 AM), https://perma.cc/B764-W3V7.

[78] INST. FOR STRATEGIC DIALOGUE, *supra* note 76, at 2.

a mass scale, COVID-19 increased the likelihood that extremist propaganda would find an audience. Security experts at the State University of New York at Albany have reported "widespread attempts by various extremists, including terrorists, to prey on the uncertainties, anxieties, and disruptions caused by the pandemic--as well as a newly captive online audience--in order to feed into and, they hope, broaden the appeal of their narratives." [79]

One white supremacist social media channel grew its user base by 800 percent in March of 2020. [80]During the first week of COVID-19 shutdowns across the United States, white supremacist content on Google saw a 13 percent increase in **[*240]** engagement. [81]Reports of anti-Asian hatred, harassment, and violence rose throughout the United States. [82]A study by the Asian Pacific Policy and Planning Council and Chinese for Affirmative Action found more than 2,000 anti-Asian incidents in the first three months of COVID-19 alone. [83]An Asian woman in California was spit on by a man who also yelled for a bus to run her over. [84]In Wisconsin, police arrested a man who allegedly harassed Asian customers for wearing protective masks while shopping. [85]And a study of Twitter hashtags between February and April of 2020 found a 300 percent increase in tweets encouraging or inciting violence against China or Chinese people. [86]Forty-three percent of those tweets originated in the United States. [87]

COVID-19 also breathed new life into anti-government conspiracies and anti-government violence. The U.S. Department of Homeland Security warned that "anti-government and anti-authority violent extremists could be motivated to conduct attacks in response to perceived infringement of liberties and government overreach as all levels of government seek to limit the spread of the coronavirus that **[*241]** has caused a worldwide pandemic." [88]The "boogaloo" ideology is a prescient example. Boogaloo is an evolving far-right movement whose followers believe a coming civil war is necessary to overthrow what they believe is a tyrannical U.S.

---

[79] Ackerman & Peterson, *supra* note 64, at 61.

[80] Billy Perrigo, *White Supremacist Groups Are Recruiting with Help from Coronavirus--And a Popular Messaging App*, TIME (Apr. 8, 2020, 4:42 PM), https://perma.cc/M8AV-8CPA ("One white supremacist channel specifically focused on messaging related to COVID-19 grew its user base from just 300 to 2,700 in that month alone--a growth of 800 [percent].").

[81] MOONSHOT, COVID-19: THE IMPACT OF SOCIAL DISTANCING ON ENGAGEMENT WITH VIOLENT EXTREMIST CONTENT ONLINE IN THE UNITED STATES 1 (2020), https://perma.cc/MDZ9-R7D6 (PDF) ("There is a shift in white supremacist search traffic across the United States the week commencing March 30th, 2020, which aligns with the implementation of 'stay at home' directives for most states.").

[82] *Reports of Anti-Asian Assaults, Harassment and Hate Crimes Rise as Coronavirus Spreads*, ANTI-DEFAMATION LEAGUE (June 18, 2020), https://perma.cc/8L8D-F6W8.

[83] Erin Donaghue, *2,120 Hate Incidents Against Asian Americans Reported During Coronavirus Pandemic*, CBS NEWS (July 2, 2020, 1:57 PM), https://perma.cc/NK78-C76M.

[84] Sabrina Tavernise & Richard A. Oppel, Jr., *Spit On, Yelled At, Attacked: Chinese-Americans Fear for Their Safety*, N.Y. TIMES (Mar. 23, 2020), https://perma.cc/A7GC-5KPG (updated June 2, 2020).

[85] Kristine Phillips, *'We Just Want to Be Safe': Hate Crimes, Harassment of Asian Americans Rise Amid Coronavirus Pandemic*, USA TODAY (May 20, 2020, 5:17 PM), https://perma.cc/P27F-WUYV (last updated May 21, 2020).

[86] MOONSHOT, FROM #CORONAVIRUSCOVERUP TO #NUKECHINA: AN ANALYSIS OF CONSPIRACY THEORIES, HATE SPEECH AND INCITEMENTS TO VIOLENCE ACROSS TWITTER RELATED TO COVID-19, at 2, 4 (2020), https://perma.cc/7VWZ-N73U (PDF).

[87] *Id.* at 3.

[88] U.S. DEP'T OF HOMELAND SEC., HOMELAND THREAT ASSESSMENT: OCTOBER 2020, at 19 (2020), https://perma.cc/6PYE-Y9RV (PDF).

government. [89]The movement gained traction on social media following government implementation of COVID-19 public health restrictions. [90]A central narrative of the boogaloo movement has been "[t]he function of COVID-19 as a tool, used by the U.S. government and law enforcement, to further infringe public freedoms under the guise of emergency response." [91]With people stuck at home during COVID-19, the boogaloo movement found a captive audience and shifted focus from extreme gun rights to COVID-19 restrictions as examples of government tyranny. [92]One boogaloo follower allegedly shot two security officers during a protest against police violence at a California courthouse, killing one of the officers. According to law enforcement, a week later, the boogaloo follower ambushed police who were executing a search warrant at his home, killing one police officer and injuring another. [93]

Then, in October, federal and state police in Michigan arrested thirteen men for plotting to storm the Michigan state capitol and kidnap Governor Gretchen Whitmer. [94]Seven of the men appeared to be boogaloo adherents who organized into a militia called the "Wolverine Watchmen" under the leadership of a person whose online persona was "Boogaloo Bunyan." Law enforcement alleged that the

> Wolverine Watchmen ha[d] called on members to identify law enforcement officers[’] home addresses in order to target **[*242]** the officers, ha[d] made threats of violence to instigate a civil war leading to societal collapse, and ha[d] engaged in planning and training for an operation to attack the Capitol of Michigan, and kidnap Government officials including the Governor of Michigan. [95]

In a short period of time, boogaloo followers and anti-government extremists had moved from the internet to the real world, with violent consequences.

Although the QAnon conspiracy predates COVID-19, the pandemic supercharged the conspiracy theory and its violent effects. Tweets about the QAnon conspiracy theory, which "purports that America is run by a cabal of pedophiles and Satan-worshippers who run a global child sex-trafficking operation and that President Trump is the only person who can stop them," [96]nearly doubled after COVID-19 entered the United States. [97]By March, COVID-19 was spreading through the country's third largest city, Los Angeles. To relieve the burden on local hospitals, the U.S. Navy sent USNS *Mercy* to the Port of Los Angeles to treat non-COVID-19 patients who otherwise

---

[89] Lois Beckett, *White Supremacists or Anti-Police Libertarians? What We Know About the 'Boogaloo'*, GUARDIAN (July 8, 2020, 2:44 PM), https://perma.cc/RC2K-ADXP.

[90] INST. FOR STRATEGIC DIALOGUE, *supra* note 76, at 5-6.

[91] *Id.* at 6.

[92] Alex Goldenberg, Joel Finkelstein & John Farmer, Jr., *How the Boogaloo Movement Is Turning Memes into Violent Action*, BROOKINGS INST. (June 29, 2020), https://perma.cc/5386-C9WC.

[93] *Id.*

[94] Kelly Weill, *Sixteen 'Boogaloo' Followers Have Been Busted in 7 Days*, DAILY BEAST (Oct. 9, 2020, 4:48 PM), https://perma.cc/6WQ7-LK6L.

[95] Affidavit in Support of Complaint at 1, State v. Musico, No. 2003273FY-FY (Mich. Cir. Ct. Oct. 7, 2020), https://perma.cc/67YS-FA7C(PDF).

[96] *What Is the QAnon Conspiracy Theory?*, CBS NEWS (Aug. 2, 2018, 6:00 AM), https://perma.cc/8FU3-V2JN (last updated Oct. 18, 2020).

[97] Ali Breland & Sinduja Rangarajan, *How the Coronavirus Spread QAnon*, MOTHER JONES (June 23, 2020), https://perma.cc/TK3J-THB6 ("The highest daily number of QAnon tweets documented by [a Twitter account tracking '#QAnon' tweets, '@conspiratoro,'] in 2019 was 75,349. After the onset of the US's coronavirus crisis, that figure nearly doubled, reaching a high of 147,748 tweets on April 4, 2020.").

would have been admitted to local hospitals. [98]The *Mercy* began accepting patients on March 30. Then, on March 31, a forty-four-year-old train engineer allegedly derailed a train delivering supplies to the *Mercy*. [99]According to law enforcement, the train engineer was "suspicious of the U.S.N.S. [*Mercy*] and believe[d] it had an alternate purpose **[*243]** related to . . . COVID-19 or a government takeover." [100]Although it remains unclear if the engineer followed QAnon conspiracy theories, his beliefs, statements, and actions align with QAnon. For example, QAnon believers had "celebrat[ed] the [U.S.] Navy's deployment of hospital ships as a sign that the Trump administration [wa]s clawing America back from the grip of Satanic pedophile elites," [101]and the engineer told police, "People don't know what's going on here. Now they will. At night, they turn off the lights and don't let anyone in. I'm going to expose this to the world." [102]Moreover, a central theme of QAnon conspiracies is "the promise of a Great Awakening, in which the elites will be routed and the truth will be revealed." [103]The anonymous social media user behind QAnon, known only as Q, posted about the "Great Awakening" only three days before the engineer's attempted attack on the *Mercy*. [104]Following his arrest, the engineer told the FBI that he derailed the train "out of the desire to 'wake people up.'" [105]The engineer also claimed that "the whole world is watching" his actions, parroting a March 28 Q post that began by saying "the entire world is watching." [106]

In late April, a thirty-seven-year-old woman in Illinois loaded her car with eighteen knives and drove for two days, allegedly trying reach the U.S. Navy's USNS *Comfort*, which was docked in New York City to assist with COVID-19 relief. The woman had become radicalized by QAnon conspiracy theories on social media. [107]During her drive to New York City, **[*244]** the woman threatened to murder former Vice President Joe Biden, who she believed was part of a non-existent cabal of Democrats engaged in pedophilia--one of many baseless QAnon conspiracies. [108]The woman arrived at the USS *Intrepid*, apparently mistaking it for the *Comfort*, and was arrested. According to reports following her arrest, the woman's Facebook page was "filled with references to QAnon," and she had fumed about *Frazzledrip*, a non-existent video that "QAnon believers claim features [former Secretary of State Hillary] Clinton and former Clinton aide Huma Abedin murdering a child." [109]The woman variously believed a QAnon conspiracy theory that the USNS *Comfort* was being used by the Trump administration to rescue abused children

---

98 Natalie Byers, *USNS Mercy Begins Treating Patients in Los Angeles*, DEP'T DEF. (Mar. 30, 2020), https://perma.cc/7EHD-UMZ6.

99 Ivan Pereira, *Engineer Tried to Crash Train into USNS Mercy in Los Angeles: Feds*, ABC NEWS (Apr. 1, 2020, 6:35 PM), https://perma.cc/J8G4-NVVB.

100 Criminal Complaint at 6-7, United States v. Moreno, No. 20-mj-01480 (C.D. Ca. Apr. 1, 2020), ECF No. 1, https://perma.cc/EH32-TKWQ(PDF).

101 Brendan Thomas-Noone & James Holloway, *Conspiracy in the Time of Coronavirus*, U.S. STUD. CTR. (Apr. 8, 2020), https://perma.cc/TZH5-6ZXY.

102 Criminal Complaint, *supra* note 100, at 5.

103 Adrienne LaFrance, *The Prophecies of Q*, ATLANTIC (May 14, 2020), https://perma.cc/H9HV-S6V9.

104 Amarnath Amarasingam & Marc-André Argentino, *The QAnon Conspiracy Theory: A Security Threat in the Making?*, CTC SENTINEL 37, 40 (2020), https://perma.cc/W8MY-RUZF (PDF).

105 Press Release, U.S. Att'y, C.D. Ca., Train Operator at Port of Los Angeles Charged with Derailing Locomotive Near U.S. Navy's Hospital Ship Mercy (Apr. 1, 2020), https://perma.cc/N2BY-NB74.

106 Amarasingam & Argentino, *supra* note 104, at 40.

107 *Id.* at 40-41.

108 Thomas Tracy & John Annese, *Unhinged Woman Whose Facebook Posts Threatened Biden Caught With Knives Near USS Intrepid*, N.Y. DAILY NEWS (Apr. 29, 2020, 10:47 PM), https://perma.cc/F5CB-YXSK.

109 Will Sommer, *A QAnon Devotee Live-Streamed Her Trip to N.Y. to 'Take Out' Biden*, DAILY BEAST (Apr. 30, 2020, 6:46 PM), https://perma.cc/E5LU-DGU9.

from the non-existent pedophilia cabal and her own theory that the *Comfort* was being used by the non-existent cabal to hold children hostage. [110]According to researchers at the Combatting Terrorism Center at West Point, only twenty days passed between the woman's first contact with the QAnon conspiracy and her commitment to engage in violence: "It is highly likely that QAnon conspiracy theories radicalized her to an apparent desire to commit violence, in light of [past] trauma that made her vulnerable." [111]

In essence, COVID-19 has been a boon for violent extremists, white supremacists, and conspiracy theorists, who have used COVID-19 as a rallying call for followers. White supremacists had a non-white "other" to blame for the pandemic--China and people of Chinese descent. Their racism was bolstered by President Trump, who alternated between calling COVID-19 the "Chinese virus" and "kung flu." [112]

Anti-government extremists simultaneously pointed to the government's inability to mitigate COVID-19 and restrictions **[*245]** on public interactions as evidence for their cause. The Trump administration's refusal to implement a national strategy for combatting the virus and attacks on COVID-19 restrictions in Democrat-led jurisdictions nurtured anti-government extremists' belief that a civil war is necessary to protect liberty. Conspiracy theories found a population of people isolated at home, seeking a sense of community, and hungry for information to bring order to the sudden disarray caused by COVID-19. And extremist ideology egged on by national leaders opened social fissures in the United States, which have been exploited by foreign adversaries to sow fear and hatred among Americans, undermine the U.S. government, weaken the United States' credibility abroad, and influence U.S. elections. [113]

VI. Looking Forward

As threats continue to evolve, the United States government must reevaluate its national security preparedness strategies to ensure biological and non-military threats are treated with the same urgency as military and intelligence threats, regardless of who leads the executive branch.

Protecting national security from biological threats begins by rebuilding U.S. diplomatic relations. Changes in population, urbanization, and climate have increased the likelihood that zoonotic diseases will emerge, particularly in regions where those changes are most acute. [114]As the spread of COVID-19 has demonstrated, naturally occurring biological threats do not respect national boundaries. The world is increasingly interconnected, and the United States should take the lead in biopreparedness and bioresponse. That means retracting the Trump administration's intent to withdraw from the World Health Organization, developing partnerships between U.S. researchers and their international counterparts, and rebuilding global alliances centered on transparency and **[*246]** cooperation. Better diplomacy means that when the next infectious disease emerges, the United States will be prepared to work with nations around the world to contain, mitigate, or eradicate the threat.

Moreover, the federal government should reevaluate the National Security Council's role in pandemic surveillance and response planning. Health experts should have a dedicated role in setting and carrying out national security policy with regard to biothreats. One option would be to reestablish NSC's Directorate of Global Health Security and Biodefense, commonly referred to as the pandemic response team, which was created by the Obama administration

---

110 *Id.*

111 Amarasingam & Argentino, *supra* note 104, at 41.

112 David Nakamura, *With 'Kung Flu,' Trump Sparks Backlash Over Racist Language--And a Rallying Cry for Supporters*, WASH. POST (June 24, 2020, 6:13 PM), https://perma.cc/K6DX-WBCC.

113 U.S. DEP'T OF HOMELAND SEC., *supra* note 88, at 11-12; *How Russia Targets U.S. Elections, Black Workers and COVID-19, Tik-Tok: RAND Weekly Recap*, RAND BLOG (Oct. 2, 2020), https://perma.cc/9JLN-USJV.

114 Suresh V. Kuchipudi, *Why So Many Epidemics Originate in Asia and Africa*, U.S. NEWS & WORLD REP. (Mar. 4, 2020, 11:02 AM), https://perma.cc/NE6A-9TDC.

and disbanded under the Trump administration. [115]Alternatively, a president could appoint a National Security Council staff member to serve as a pandemic coordinator, whose job would be to monitor federal agencies' assessments of biological threats, report emerging biological threats to the National Security Council, and coordinate agencies' plans in the event a disease becomes an epidemic or pandemic.

Protecting the nation and its people is a core government function, but national security is achievable only if the federal government develops coordinated, comprehensive plans and has decision makers who are capable of executing those plans. President Kennedy largely got it right during the Cuban Missile Crisis. He gathered relevant data, assembled expert advisers, listened to his advisers and to Congress, settled on a strategy, and followed through with it. President Trump largely got it wrong during the COVID-19 pandemic. He ignored data and intelligence, assembled then contradicted expert advisers, sidestepped Congress, eschewed an already existing strategy, and lied to the public about the public health threat. The result--no national strategy for mitigating the effects of a pandemic, a jurisdiction-by-jurisdiction patchwork of public health policies that struggled to contain the virus, and mass anxiety that made people more susceptible to violent ideology -- compounded COVID-19's danger to U.S. national security. These proposals, whether enacted through legislation or policy making, are in no way a panacea, but they will serve as guardrails to ensure the federal government is prepared to **[*247]** follow its own national security and biodefense strategies in the event of another deadly pandemic.

Washington & Lee Law Review Online
Copyright (c) 2020 Washington & Lee University School of Law%Washington & Lee Law Review Online

---

End of Document

---

115 Reichmann, *supra* note 33.