# 1AC

#### Same as round 1

# 2AC

## T Prohibit

#### Restrict and regulate are synonymous

Paust ’08 (Mike & Teresa Baker Law Center Professor, University of Houston)

Jordan 14 U.C. Davis J. Int'l L. & Pol'y 205

The primacy of customary international law is also evident in an opinion by Justice Chase in 1800. In Bas v. Tingy, Justice Chase recognized that "if a general war is declared [by Congress], its extent and operations are only restricted and regulated by the jus belli, forming a part of the law of nations ... ." n47 Therefore, the law of nations (and, in particular, the law of war) necessarily restricts and regulates congressional authorization of war's extent and operations. n48 In 1798, Albert Gallatin had recognized similarly: "By virtue of ... [the war power], Congress could ... [act], provided it be according to the laws of nations and to treaties." n49 And in 1804, counsel had argued before the Supreme Court that "as far as Congress have thought proper to legislate us into a state of war, the law of nations in war is to apply." n50 The restrictive role of the laws of war [\*221] apparently formed the basis for Justice Story's statement in 1814 that conduct under a relevant act of Congress "was absorbed in the more general operation of the law of war" and was permissible "under the jus gentium" or law of nations. n51 Although there was no clash between the act and the laws of war, the laws of war recognizably had a higher, "more general" absorbing effect.

#### Counter-interp: Statutory restrictions are legislative limits

Law dictionary No Date

http://thelawdictionary.org/statutory-restriction/

STATUTORY RESTRICTION?

Limits or controls that have been place on activities by its ruling legislation

#### Neg interp impossible: Congress CANNOT prohibit

Colella ‘88

Frank SPRING, 1988 54 Brooklyn L. Rev. 131

Because the subsequent versions of the amendment sought to deny the executive any latitude in supporting the Contras, they seem to be examples of congressional overreaching. Congress may regulate aspects of "foreign covert action," but it cannot totally bar the president from carrying them out. n151 One commentator incisively observes, "[C]ongress cannot deny the President the capacity to function effectively in this area any more than it could deny the courts the capacity to carry out their independent constitutional duties." n152 The restrictions contained in later versions of the amendments n153 make it apparent that Congress prevented effective execution of the president's policy objectives.

## Counterplan

#### Links to politics

Goldsmith ‘13

[Jack, Washington Post, <http://articles.washingtonpost.com/2013-02-05/opinions/36757699_1_government-lawyers-secret-warfare-al-qaeda> ETB]

A new legal and political foundation for stealth warfare cannot succeed without the initiative and support of the president. The chances of such support, however, are dim. The Obama administration prefers to act based on old authorities and not to engage Congress in establishing new authorities for new wartime challenges. This is unfortunate for U.S. constitutional traditions and for the stability of our long-term counterterrorism strategy. And it is unfortunate for the president, not only because he increasingly acts without political cover, and because his secret wars are increasingly criticized and scrutinized abroad, but also because he alone will be bear the legacy of any negative consequences — at home and globally — of unilateral, lethal, secret warfare.

#### The counterplans covert action ensures unilateralism – prevents coalitions and fuels suspicion and cyberwar

**Rishikof 11**, Chair of the ABA Standing Committee on Law and National Security. Former professor of law and chair

(PROJECTING FORCE IN THE 21ST CENTURY - LEGITIMACY AND THE RULE OF LAWDepartment of National Security Strategy, National War Collegwww.rutgerslawreview.com/wp-content/uploads/archive/vol63/Issue4/Mustin-Rishikof\_Article\_PDF.pdf)

**Covert action** also **enables unilateral action. The stealthy nature of covert action means that the Executive would be discouraged from seeking international cooperation**. Any international support would likely be limited to notifying host nations of the presence of troops, and those notifications, as a tactical matter, would likely be last minute and very directive in nature. **This type of unilateral action** contrasts the cooperative intent for international law, and, in the words of one legal scholar, ―[u]nilateral action- covert or overt - **generates particularly high emotions, because many view it as a litmus test for one‘s commitment to international law. Excessive use of covert action might be deemed** by some nations **as a rebuke of international law or evidence of a hubristic foreign policy**. **The** continued and constant **use of this instrument** when lethality is the goal **raises issues of international legitimacy.**

#### Covert designation fuels suspicion and can’t solve cyber war — also removes international pressure from Chinese hacking

**Wright 11**, Executive director of studies at The Chicago Council on Global Affairs

(Thomas, 6/26, America has double standards in fighting cyberwar, [www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w](http://www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w))

While it has several advantages, **treating American cyber-destruction as a covert operation will severely undermine the new cyber-strategy. Suspicion that the US uses cyber­weapons whenever convenient will hamper its attempts to press other states to be transparent about their intentions**. **In particular, it takes the pressure off China, widely believed to be the leading state source of cyberattacks. It may also dissuade the US from developing the technology to trace the source of an attack.**

#### Nuclear war

**Sirota, Best-Selling Author, 11**, David Sirota is a best-selling author of the new book "Back to Our Future: How the 1980s Explain the World We Live In Now.", The Terrorist Threat We’re Ignoring, http://www.salon.com/news/david\_sirota/2011/07/11/trade\_terrorism

All of these threats are, indeed, scary -- and the last one, which sounds like something out of "Saw" movie, is especially creepy. But the fear of individual terrorist acts has diverted attention from a more systemic threat that is taking the implant idea to a much bigger platform. I'm talking about the threat of terrorists or foreign governments exploiting our economy's penchant for job outsourcing/offshoring. How? By using our corresponding reliance on imports to secretly stitch security-compromising technology into our society's central IT nervous system. Sounds far-fetched, right? Sounds like some fringe theory bizarrely melding liberal political complaints about bad trade policies with tinfoil-hat paranoia, right? Yeah, that's what I thought, until last week when -- in an announcement largely ignored by the Washington press corps -- the Department of Homeland Security made a stunning disclosure at a congressional hearing. As the business trade publication Fast Company [reports](http://www.fastcompany.com/1765855/dhs-someones-spiking-our-imported-tech-with-attack-tools) (emphasis added): A top Department of Homeland Security (DHS) official has admitted on the record that electronics sold in the U.S. are being preloaded with spyware, malware, and security-compromising components by unknown foreign parties. In testimony before the House Oversight and Government Reform Committee, acting deputy undersecretary of the DHS National Protection and Programs Directorate Greg Schaffer told Rep. Jason Chaffetz (R-UT) that both Homeland Security and the White House have been aware of the threat for quite some time. When asked by Rep. Chaffetz whether Schaffer was aware of any foreign-manufactured software or hardware components that had been purposely embedded with security risks, the DHS representative stated that "I am aware of instances where that has happened," after some hesitation. This supply chain security issue essentially means that, somewhere along the line, technology being marketed in the United States was either compromised or purposely designed to enable cyberattacks. The process by which this happens is fairly straightforward -- and its connection to our tariff-free trade policies that encourage outsourcing is obvious. First, an American company or governmental agency orders a piece of computer hardware or software from a tech company. Then, because the "free" trade era has economically incentivized those companies to move their production to low-wage countries, much of that order is actually fulfilled at foreign facilities where security and quality standards may be, ahem, lacking. If this still sounds far-fetched, remember that in the offshoring/outsourcing epoch, one of the major exporters of computer hardware -- and increasingly, software -- is China. That is, the country whose government has been at the forefront of aggressively researching, developing and implementing covert technologies that turn computers into stealth weapons of the police state. There is, for example, China's Great Firewall, which prevents computers from accessing content the government deems unacceptable. There's also the [Green Dam initiative](http://online.wsj.com/article/SB124638689078074805.html), which aimed to preload spying and censorship software on PCs. These, of course, are just the cyber-sabotage projects we know about, suggesting that there are far more being engineered by the Chinese regime. And this says nothing of the additional possibility of stateless terrorist groups infiltrating the high-tech supply chain to invisibly weave vulnerabilities into our IT infrastructure. If you think the biggest ramifications of this threat are merely Angry Birds malfunctions, suddenly shitty pictures from Hipstamatic and yet longer wait times when you fire up Microsoft Word -- think again. In an information age that sees [missiles remotely fired via keystrokes](http://news.cnet.com/8301-11386_3-10064231-76.html) and data mined for intelligence gathering, supply chain vulnerabilities in high-tech products are a genuine national security problem. Indeed, they are at least as big a threat to national security as the old concerns about how, say, offshoring steel production could compromises our strength by limiting our ability to unilaterally build tanks and warships. By creating a trade policy that helps offshore high-tech production, we may be inadvertently importing spying or terrorist instruments and then embedding those instruments into our computer-dependent society at large. What might this mean in practice? As the U.S.-China Economic and Security Review Commission [reported](http://www.nextgov.com/nextgov/ng_20110707_5612.php?oref=topstory) a few months ago, it could be "kill switches" implanted in Pentagon systems that **control our arsenal**. It could be new "War Games"-esque back doors that allow Chinese military hackers to punch in their own preprogrammed "Joshua" password and [again](http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html) breach computer networks deep within our national security apparatus.

#### 2. CP Fails

Scheuerman 12 – William E. Scheuerman, Professor of Political Science and West European Studies at Indiana University, "Review Essay:  Emergencies, Executive Power, and the Uncertain Future of US Presidential Democracy", Law and Social Inquiry, Summer, 37 Law 26 Soc. Inquiry 743, Lexis

Posner and Vermeule rely on two main claims. First, even if the president constitutes the dominant actor in a legally unchecked administrative state, he or she has to gain elite and public support to get things done and stand for election. So how can political actors decide whether or not the executive is performing well? Posner and Vermeule tend to hang their hats on “executive signaling”: presidents can send signals to voters communicating that they are “well-motivated,” and that in fact many voters might make the same (or at least similar) decisions if they possessed the information the president typically has. By communicating in a certain way (e.g., by appointing members of the opposing party to his or her cabinet, promising to accept the recommendations of an independent commission, or by making decisions as transparent as possible), presidents can gain credibility, and voters might thereby come to acknowledge the plausibility—if not necessarily the substantive rightness—of what the executive is doing (2010, 137–53).¶ However, as Schmitt aptly grasped, even formally free elections potentially become charades when the executive effectively exercises legally unconstrained power (e.g., in Peronist Argentina, or Putin's Russia). Posner and Vermeule never really provide enough evidence for us to dismiss this possibility. Since the president in our system is only subject on one occasion to reelection, it is unclear how their proposals might meaningfully check the executive, particularly during a second term. The fact that executive signaling represents a form of self-binding hardly seems reassuring, either (2010, 135). Nor does the book's highlighting of the possible dangers of different forms of executive signaling (e.g., too much transparency, or an excessive subservience to independent agencies) help very much on this score (2010, 142–46). Why should we expect to get presidents who know how to engage in executive signaling in just the right way?¶ The familiar reason the executive needs elite and popular support, of course, is that it still relies on a popularly elected Congress and other institutional players to get things done: this is why describing such dependence as intrinsically political and “nonlegal” seems odd. For that matter, the relationship between what we traditionally have described as a normative theory of political legitimacy and executive signaling mechanisms—whereby the executive gains popular credibility—remains ambiguous. Is their theory of executive signaling and credibility meant to stand in for a normative theory of legitimacy? If so, one might worry. We can easily imagine an executive diligently doing many of the things prescribed here yet nonetheless pursuing policies deeply at odds with the common good, or at least with what a democratic community under more ideal conditions might determine to be in its best interests. Depending on one's normative preferences, some of the examples provided of executive signaling (e.g., FDR and Obama naming Republicans to their cabinets) might legitimately be taken as evidence for presidential Machiavellianism, rather than as solid proof that the presidents in question were well-motivated and thereby somehow politically acceptable. Presidential “signaling” seems like a pale replacement for liberal legalism and the separation of powers.

#### 3. Plan’s way more credible **Pildes 12** – Richard H. Pildes, Sudler Family Professor of Constitutional Law at the NYU School of Law and Co-Director of the NYU Center on Law and Security, "Book Review: Law and the President", Harvard Law Review, April, 125 Harv. L. Rev. 1381, Lexis

That Posner and Vermeule miss the role of legal compliance as a ¶ powerful signal, perhaps the most powerful signal, in maintaining a ¶ President’s critical credibility as a well-motivated user of discretionary ¶ power is all the more surprising in light of the central role executive ¶ self-binding constraints play in their theory. After asserting that “one ¶ of the greatest constraints on [presidential] aggrandizement” is “the ¶ president’s own interest in maintaining his credibility” (p. 133), they ¶ define their project as seeking to discover the “social-scientific ¶ microfoundations” (p. 123) of presidential credibility: the ways in ¶ which presidents establish and maintain credibility. One of the most ¶ crucial and effective mechanisms, in their view, is executive selfbinding, “whereby executives commit themselves to a course of action ¶ that would impose higher costs on ill-motivated actors” (p. 137). As ¶ they also put it, “a well-motivated president can distinguish himself ¶ from an ill-motivated president by binding himself to a policy position ¶ that an ill-motivated president would reject” (p. 135). ¶ By complying with these constraints, presidents signal their good ¶ faith and accrue more trust to take further action. Most importantly ¶ from within Posner and Vermeule’s theory, these constraints, many ¶ self-generated through executive self-binding, substitute for the constraints of law. Law does not, or cannot, or should not constrain presidents, in their view, but rational-actor presidents recognize that complying with constraints is in their own self-interest; presidents ¶ therefore substitute or accept other constraints. Thus, Posner and ¶ Vermeule recognize the importance of “enabling constraints”78 in effective mobilization and maintenance of political power; that is, they recognize that what appear to be short-term constraints on the immediate ¶ preferences of actors like presidents might actually enable long-term ¶ marshaling of effective presidential power. Yet they somehow miss ¶ that law, too, can work as an enabling constraint; when it comes to ¶ law, Posner and Vermeule seem to see nothing but constraint. Indeed, ¶ this failing runs even deeper. For if presidents must signal submission ¶ to various constraints to maintain and enhance their credibility — as ¶ Posner and Vermeule insist they must — Posner and Vermeule miss ¶ the fact that the single most powerful signal of that willingness to be ¶ constrained, particularly in American political culture, is probably the ¶ President’s willingness to comply with law.

#### 4. Links to politics – congress wants to be involved

Sasso 2012

(Brandon Sasso, December 21, 2012, “House Republicans urge Obama not to issue cybersecurity order,” The Hill, http://thehill.com/blogs/hillicon-valley/technology/274391-house-republicans-urge-obama-not-to-issue-cybersecurity-order)

A group of 46 House Republicans, led by Reps. Marsha Blackburn (Tenn.) and Steve Scalise (La.), sent President Obama a letter on Friday urging him not to issue an executive order on cybersecurity.¶ "Instead of preempting Congress' will and pushing a top-down regulatory framework, your administration should engage Congress in an open and constructive manner to help address the serious cybersecurity challenges facing our country," the lawmakers wrote. ¶ The White House is currently drafting an executive order that would encourage operators of critical infrastructure, such as banks and electric grids, to meet cybersecurity standards. ¶ The administration says the order, which could come as early as January, is necessary to protect vital systems from hackers.¶ The White House began working on the order after Senate Republicans blocked the Democrats' preferred cybersecurity bill.¶ But in their letter, the House Republicans urged the administration to continue working with Congress.

## OCOs Good DA

#### Non-unique — cyber arms race and use is inevitable now — I did that analysis on case — it’s try or die for a restrained strategy — active defense causes Cyberwar

McGraw 12**,** Member of the IEEE Computer Society Board of Governors, Gary McGraw is a recognized authority on software security. He is an author of many books and over a 100 [peer-reviewed](http://en.wikipedia.org/wiki/Peer-reviewed) publications in this field, authors a monthly security column for [informIT](http://en.wikipedia.org/wiki/InformIT), and is an editor of Addison-Wesley Software Security series. In addition, Gary McGraw serves on the Dean’s Advisory Council for the School of Informatics of Indiana University, and produces the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine (syndicated by informIT). Gary is the Chief Technical Officer at [Cigital Inc.](http://en.wikipedia.org/wiki/Cigital) In addition, he serves on the advisory boards of several companies, including [Dasient](http://en.wikipedia.org/wiki/Dasient), [Fortify Software](http://en.wikipedia.org/wiki/Fortify_Software), Invincea, and Raven White. He holds dual PhD in Cognitive Science and Computer Science from Indiana University. In the past, Gary McGraw has served on the [IEEE Computer Society](http://en.wikipedia.org/wiki/IEEE_Computer_Society) Board of Governors.

Creating a cyber-rock is cheap. Buying a cyber-rock is even cheaper since zero-day attacks exist on the open market for sale to the highest bidder. In fact, if the bad guy is willing to invest time rather than dollars and become an insider, cyber-rocks may in fact be free of charge, but that is a topic for another time. Given these price tags, it is safe to assume that some nations have already developed a collection of cyber-rocks, and that many other nations will develop a handful of specialized cyber-rocks (e.g., as an extension of many-year-old regional conflicts). If we follow the advice of Hayden and Chabinsky, we may even distribute cyber-rocks to private corporations. Obviously, active defense is folly if all it means is unleashing the cyber-rocks from inside of our glass houses since everyone can or will have cyber-rocks. Even worse, unlike very high explosives, or nuclear materials, or other easily trackable munitions (part of whose deterrence value lies in others knowing about them), no one will ever know just how many or what kind of cyber-rocks a particular group actually has. Now that we have established that cyber-offense is relatively easy and can be accomplished on the cheap, we can see why reliance on offense alone is inadvisable. What are we going to do to stop cyberwar from starting in the first place? The good news is that war has both defensive and offensive aspects, and understanding this fundamental dynamic is central to understanding cyberwar and deterrence. The kind of defense I advocate (called "passive defense" or "protection" above) involves security engineering -- building security in as we create our systems, knowing full well that they will be attacked in the future. One of the problems to overcome is that exploits are sexy and engineering is, well, not so sexy.

**Deterrence doesn’t apply to cyberspace**

**Weiner 12, research intern for the Project on Nuclear Issues**, Boss, Internally cites Dr. Lewis who is the director of the Center for Homeland Security and Defense, <https://www.hsdl.org/hslog/?q=node/9216> \*\*Note: Sarah Weiner is Cal debate coach, however this evidence relies upon Dr. Lewis’s findings and was written before the announcement of the topic \*\*

Others vehemently disagree with this presupposition. Jim Lewis, for example, [argued](http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/) earlier this month at an event at the Stimson Center that **deterrence will not work in the cyber domain**. He emphasized that difficulties in attributing attacks, “holding hostage” adversaries’ cyber and physical assets, and achieving a proportional response all decrease the credibility of US threats and reduce the costs of an adversaries’ hostile cyber operations. And Dr. Lewis has considerable evidence on his side: public and private entities in the US experience cyber-attacks on a daily basis. If these attacks are deterrable, **we are doing a terrible job** of leveraging our capabilities. For a number of reasons, trying to apply nuclear deterrence logic to cyber warfare feels a bit too much like trying to fit a square peg into a round hole. That does not mean, however, that we should abandon all attempts to draw analogies between cyber and nuclear strategy. Despite a few close calls, the basic principles of nuclear deterrence and mutually assured destruction have prevented the use of nuclear weapons for over 60 years. Understanding the reason why this largely effective and stable model of deterrence cannot map cleanly onto the cyber world may help us better conceptualize strategies for cyber-deterrence. The first difficulty is establishing an analogue between a nuclear attack and a cyber-attack. We know when a nuclear bomb explodes, and we know it is unacceptable. The spectrum of cyber-attacks, however, spans far, far below the destructiveness of a nuclear strike. Denial-of-service attacks, such as Iran’s [recent shutdown](http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html) of several banks’ websites, are a world away from the detonation of any weapon, not to mention a nuclear weapon. This creates the problem of credibility and proportionality Dr. Lewis spoke about: responding to such low-level attacks with a military use of force is so disproportionate that it is not a credible threat. ¶ If the US instead decides to use cyber capabilities to deter cyber-attacks, it runs into a second problem. Cyber “weapons” cannot be used in the same way we use nuclear weapons because, unlike nuclear weapons, the demonstration of a cyber-capability quickly renders that capability useless. If the US were to release the details of a cyber-weapon, intended to signal a retaliatory capability, potential adversaries could attempt to steal the technology and/or harden their cyber defenses against the US weapon’s specific attributes. This is the opposite of nuclear deterrence, in which the US pursues the most credible and reliable force so that other nations know precisely how damaging a US counterstrike would be. Demonstrating that a nation could effectively mount a second-strike in response to a nuclear attack creates a stabilizing dynamic of mutually assured destruction in which no nation believes it could gain militarily by launching a nuclear attack. The trouble with cyber weapons, however, is that they cannot be so transparently deployed. **The only effective cyber-attack is an unexpected attack, and that does nothing for signaling or deterrence.**

**Otherwise organizational confusion OCOs fail**

**GAO 11**, Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities, <http://www.gao.gov/assets/330/321824.html>

DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both its own command and a geographic combatant command. Without complete and clearly articulated guidance on command and control responsibilities that is well communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyberspace operations.

**Turn — Miscalc — only the plan solves deterrence failures**

**Lord et al 11, Vice President and Director of Studies at the Center for a New American Security**

(Kristin M., Travis Sharp is the Bacevich Fellow at the Center for a New American Security. Joseph S. Nye, Jr. is University Distinguished Service Professor at the Kennedy School of Government at Harvard University. Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. Nathaniel Fick is Chief Executive Officer of the Center for a New American Security. Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University. David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. M. Ethan Lucarelli is an Associate at Wiley Rein LLP. Roger H. Miksad is an Associate at Wiley Rein LLP. James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. Richard Fontaine is a Senior Fellow at the Center for a New American Security. Will Rogers is a Research Associate at the Center for a New American Security. Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors, “America’s Cyber Future Security and Prosperity in the Information Age volume I” June 2011, [http:// www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf))

The **Department of Defense**, the **intelligence community**, the Department of **Justice, Congress and the White House should** **clarify** legal **authorities** related to military and intelligence operations in cyberspace. GEN Alexander told Congress in March 2011 that the U.S. military does not yet possess the legal authorities it needs to respond to a cyber attack against the United States or its allies.197 LtGen Robert Schmidle, Jr., deputy commander of Cyber Command, elaborated that “**There is a real dearth of doctrine and policy** in the world of cyberspace,” **pointing to the lack of coordination and guidance from civilian leadership**.198 This **lack of clarity is understandable** as cyber operations evolve faster than legal and political processes, but it could **cause confusion and disorganization during a major cyber attack**. By **delineating the authorities granted** to the military, the U.S. government **will reduce uncertainty and** thereby **increase its ability to use the capabilities** it has more effectively and **without undue hesitati**on. This outcome will **raise the retaliatory costs suffered by potential adversaries** if they attack the United States and the attacks can be attributed to them, which **will help deter them in the first place**.

**Turn — organization confusion dooms OCOs now — only statutory legislation solves**

**Chesney 12**, **Charles I. Francis Professor in Law, University of Texas School of Law**, Military-Intelligence Convergence and the Law of the Title 10 Title 50 debate, <http://jnslp.com/wp-content/uploads/2012/01/Military-Intelligence-Convergence-and-the-Law-of-the-Title-10Title-50-Debate.pdf>

That architecture is a complex affair, including what might be described as “framework” statutes and executive branch directives generated in fits and starts over the past forty years. Ideally, it serves to mediate the tension between the desire for flexibility, speed, and secrecy in pursuit of national defense and foreign policy aims, on one hand, and the desire to preserve a meaningful degree of democratic accountability and adherence to the rule of law, on the other. Of course, the legal architecture has never been perfect on this score, or even particularly close to perfection. But the convergence trend has made the current architecture considerably less suited towards these ends. First, it reduces the capacity of the existing rules to promote accountability. The existing rules attempt to promote accountability in two ways. They promote it within the executive branch by requiring explicit presidential authorization for certain activities, and they promote accountability between the executive branch and Congress by requiring notification to the legislature in a broader set of circumstances. Convergence undermines these rules by exposing (and exacerbating) the incoherence of key categorical distinctions upon which the rules depend, including the notion that there are crisp delineations separating intelligence collection, covert action, and military activity. As a result, it is possible, if not probable, that a growing set of exceptionally sensitive operations – up to and including the use of lethal force on an unacknowledged basis on the territory of an unwitting and non-consenting state – may be beyond the reach of these rules. Second, the convergence trend undermines the existing legal architecture along the rule-of-law dimension by exposing latent **confusion and disagreement** regarding which substantive constraints apply to military and intelligence operations. Is international law equally applicable to all such operations? Is an agency operating under color of “Title 50” at liberty to act in locations or circumstances in which the armed forces ordinarily cannot? These questions are not in fact new, but thanks to convergence they are increasingly pressing. Government lawyers are well aware of these issues, and in fact have been grappling with them for much of the past decade, if not longer.5 For many years, however, public reference to them was quite limited. The most important early post-9/11 example came in 2003, when The Washington Times reported that the Senate Select Committee on Intelligence was quietly attempting to expand its oversight authority in order to encompass certain clandestine military operations in response to concern about the expanding role of special operations units in the war on terrorism.6 That effort failed in the face of fierce pushback from the Pentagon and the Senate and House Armed Services Committees,7 but not before drawing at least some attention to the disruptive impact convergence even then was having on the accountability system.8 In more recent years, the media has begun to pay more sustained attention, frequently noting that the complications associated with convergence impact question of substantive authority as well as accountability. In 2010, for example, The Washington Post reported that a fierce interagency debate was underway in connection with “which agency should be responsible for carrying out attacks” online, with the CIA categorizing certain attacks as covert actions which are “traditionally its turf” and the military taking the position that such operations are “part of its mission to counter terrorism, especially when, as one official put it, ‘alQaeda is everywhere.’”9 And the same Washington Post story indicated that the Justice Department’s Office of Legal Counsel had produced a draft opinion in spring 2010 “that avoided a conclusive determination on whether computer network attacks outside battle zones were covert or not,” but that nonetheless concluded that “[o]perations outside a war zone would require the permission of countries whose servers or networks might be implicated.”10 Subsequent stories about the use of lethal force in Yemen have also raised the issue of host-state permission, suggesting that JSOC but not the CIA would be obliged to act only with such permission, and that as a result JSOC units might at times prefer to operate under color of the CIA’s authority11 (as happened in Pakistan with Osama bin Laden, and again in Yemen with Anwar al-Awlaki).12 These accounts give a sense of the range of legal questions that convergence generates, as well as the debates that surround them within the government. And that in turn is enough to frame the investigation that follows. I proceed in two parts, beginning in Part I with a descriptive account of the convergence trend itself. Part I opens with a focus on events in the 1980s and 1990s that presaged the accelerated convergence of the post-9/11 period. Attempts by the military to develop within the special forces community capacities quite similar to those of the CIA are described in Part I.A, and CIA flirtations with the use of deadly force against terrorists are described in Part I.B. Against that backdrop, Part I.C. then explores how convergence has manifested over the past decade, with an emphasis on the CIA’s kinetic turn, JSOC’s parallel expansion, the development of hybrid CIA-JSOC operations, and the emergence of cyberspace as an operational domain. Readers already familiar with the convergence phenomenon may wish to skip ahead to Part II, which examines the impact of convergence on the domestic legal architecture relevant to such activities.13 Part II.A. clarifies what I have in mind when I refer to a domestic legal architecture, as it traces the emergence and growth of standing rules relating to (i) the internal executive branch decisionmaking process, (ii) information-sharing between the executive branch and Congress, and (iii) substantive authorizations and prohibitions relating to certain types of activity. The remainder of Part II analyzes the impact of convergence on each of these rules, demonstrating the manner in which convergence creates new problems for (and exacerbates existing problems in) the existing legal architecture. The key issues include: the increasingly large and significant set of military operations that are not subject to either presidential authorization or legislative notification; lingering suspicion with respect to what law if any restrains the CIA’s use of lethal force; confusion with respect to whether and why the CIA might be at greater liberty than JSOC to conduct operations without host-state consent; and the difficulty of mapping the existing architecture onto operations conducted in cyberspace. I embed my recommendations for reform within the analysis at each step along the way. To summarize, I offer four recommendations. Enhance Accountability within the Executive Branch. The current legal architecture requires presidential approval for “covert action” programs, but the situation is complicated with respect to unacknowledged military operations. An unacknowledged military operation must be authorized by the President or at least the Secretary of Defense if it is collateral to an anticipated overt military operation that is not yet imminent but for which operational planning has been authorized – a sweeping set of circumstances. But no such approval is required if the operation is collateral to ongoing hostilities. This makes sense if the unacknowledged operation occurs in the combat zone. If it occurs on the territory of another state outside the “hot” battlefield, however, the risks are sufficient to warrant extension of the requirement of presidential or at least secretarial authorization. Notably, press accounts indicate that former Secretary of Defense Robert M. Gates had insisted upon such an approach for lethal operations outside the hot battlefield, as a matter of policy. At a minimum, that policy should be codified. Better still to extend it to all unacknowledged military operations outside the combat zone. The degree of accountability involved should be commensurate with the risks, and in light of convergence there is little reason to calibrate that judgment differently for the military than for the CIA, at least not outside combat zones. Enhance Information-Sharing with Congress. Operations constituting “covert action” must be reported to the House and Senate Intelligence Committees; by contrast, the unacknowledged military operations discussed above are not subject to this requirement. A separate law requires notification to Congress when the armed forces are deployed in circumstances involving a likelihood of hostilities, but given the strict interpretation of “hostilities” adopted in relation to the conflict in Libya it seems clear that a considerable amount of unacknowledged military activity might escape notification to Congress under that regime as well. An effort was made in 2003 to close this gap by requiring unacknowledged military activity to be reported to the Intelligence Committees when activity occurs outside the geographic confines of a state where the United States has an overt combat presence. The effort failed in the face of resistance from the Pentagon and the House and Senate Armed Services Committees. It should be revived, but with notification being made to the Armed Services Committees, subject to an option for close-hold notifications, based on the Gang of Eight model. All such notification scenarios should be modified, however, to include participation by the chief majority and minority counsels of the relevant committees (creating, in effect, a “Gang of Twelve” system). Clarify Substantive Constraints on Title 50 Operations. It should be made clear that all U.S. government agencies comply with the law of war in any operation to which the law of war applies, regardless of whether the operation is categorized as a Title 10 or a Title 50 activity and regardless of which particular agency carries it out. This is not necessarily a change from current policy, but it would help to address concerns that critics have raised with respect to whether the CIA conforms its drone operations to law of war standards. On the other hand, it would not be appropriate to adopt a similar express commitment vis-a-vis international law’s treatment of state sovereignty, given lingering uncertainty with respect to whether and when international law prohibits one state from conducting espionage, covert action, or other operations within another state’s territory in the first place.

## Iran Sanctions Politics DA

1. **Forcing controversial fights key to Obama’s agenda—the alt is gridlock**

John **Dickerson**, Slate, **1/18/13,** Go for the Throat!, [www.slate.com/articles/news\_and\_politics/politics/2013/01/barack\_obama\_s\_second\_inaugural\_address\_the\_president\_should\_declare\_war.single.html](http://www.slate.com/articles/news_and_politics/politics/2013/01/barack_obama_s_second_inaugural_address_the_president_should_declare_war.single.html), CMR

On Monday, President Obama will preside over the grand reopening of his administration. It would be altogether fitting if he stepped to the microphone, looked down the mall, and let out a sigh: so many people expecting so much from a government that appears capable of so little. A second inaugural suggests new beginnings, but this one is being bookended by dead-end debates. **Gridlock** over the fiscal cliff **preceded** it and **gridlock** over the debt limit, sequester, and budget will follow. After the election, **the same people are in power in all the branches of government and they don't get along. There's no indication that** the president's **clashes with** House Republicans **will end soon**. Inaugural speeches are supposed to be huge and stirring. Presidents haul our heroes onstage, from George Washington to Martin Luther King Jr. George W. Bush brought the Liberty Bell. They use history to make greatness and achievements seem like something you can just take down from the shelf. Americans are not stuck in the rut of the day. But this might be too much for Obama’s second inaugural address: After the last four years, how do you call the nation and its elected representatives to common action while standing on the steps of a building where collective action goes to die? That bipartisan bag of tricks has been tried and it didn’t work. People don’t believe it. Congress' approval rating is 14 percent, the lowest in history. In a December Gallup poll, 77 percent of those asked said the way Washington works is doing “serious harm” to the country. **The challenge for** President **Obama’s** speech is the challenge of his **second term: how to be great when the environment stinks. Enhancing the president’s legacy requires** something **more than** simply the clever application of **predictable stratagems**. Washington’s **partisan rancor**, the size of the problems facing government, **and the limited amount of time before Obama is a lame duck all point to a single conclusion: The president** who came into office speaking in lofty terms about bipartisanship and cooperation **can only cement his legacy if he destroys the GOP**. If he wants to transform American politics, **he must go for the throat**. President Obama could, of course, resign himself to tending to the achievements of his first term. He'd make sure health care reform is implemented, nurse the economy back to health, and put the military on a new footing after two wars. But he's more ambitious than that. He ran for president as a one-term senator with no executive experience. In his first term, he pushed for the biggest overhaul of health care possible because, as he told his aides, he wanted to make history. He may already have made it. There's no question that he is already a president of consequence. But there's no sign he's content to ride out the second half of the game in the Barcalounger. He is approaching gun control, climate change, and immigration with wide and excited eyes. He's not going for caretaker. How should the president proceed then, if he wants to be bold? The Barack **Obama** of the first administration **might have approached the task by finding** some **Republicans to deal with and** then start agreeing to some of their demands in hope that he would **win some of their votes**. It's the traditional approach. Perhaps he could add a good deal more schmoozing with lawmakers, too. **That's the old way. He has abandoned that.** **He doesn't think it will work** and **he doesn't have the time.** As Obama explained in his last press conference, he thinks the **Republicans are dead set on opposing him**. **They cannot be unchained by schmoozing**. **Even if Obama were wrong about Republican intransigence, other constraints will limit the chance for cooperation**. **Republican lawmakers worried about primary challenges** in 2014 **are not going to be willing partners.** He probably has at most 18 months before people start dropping the lame-duck label in close proximity to his name. **Obama’s only remaining option is to pulverize**. Whether he succeeds in passing legislation or not, given his ambitions, his goal should be to delegitimize his opponents. **Through a series of clarifying fights over controversial issues, he can force Republicans to** either side with their coalition's most extreme elements or **cause a rift in the party that will leave it**, at least temporarily, **in disarray**.

1. **No link — the plan’s not controversial**

**Perera 6/26**, SACS calls for new oversight of Cyber Command, David Perera is executive editor of the FierceMarkets Government Group, which includes FierceGovernment, FierceGovernmentIT, FierceHomelandSecurity, and FierceMobileGovernment. He has reported on all things federal since January 2004 and is co-author of [Inside Guide to the Federal IT Market](http://store.brightkey.net/mconcepts_ebiz/OnlineStore/ProductDetail.aspx?ProductId=201530), a book published in October 2012., <http://www.fiercegovernmentit.com/story/sasc-calls-new-oversight-cyber-command/2013-06-26>

The Senate Armed Services Committee says it has concerns that oversight of Cyber Command and the cyber mission within the Defense Departments "is fragmented and weak," calling for creation of a Senate-confirmed position within the undersecretary of defense for policy to supervise and manage the funds of offensive cyber forces.

**The Senate committee voted 23-3** on June 14 to report its version of the fiscal 2014 national defense authorization act ([S. 1197](http://hdl.loc.gov/loc.uscongress/legislation.113s1197)), detailing its intentions in a newly released legislative [report](http://www.gpo.gov/fdsys/pkg/CRPT-113srpt44/pdf/CRPT-113srpt44.pdf)(.pdf).

1. **Plan’s super popular**

**Bradbury 11**, Steven G. Bradbury is an attorney at the Washington, D.C office of [Dechert LLP](http://en.wikipedia.org/wiki/Dechert_LLP).

Bradbury was head of the [Office of Legal Counsel](http://en.wikipedia.org/wiki/Office_of_Legal_Counsel) (OLC) in the [United States Department of Justice](http://en.wikipedia.org/wiki/United_States_Department_of_Justice) during the [George W. Bush administration](http://en.wikipedia.org/wiki/George_W._Bush_administration), 2005-January 2009. Appointed the Principal Deputy Assistant Attorney General for OLC in April 2004, he became the Acting Assistant Attorney General in 2005. He was nominated by President [George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush) to be the Assistant Attorney General for OLC in June 2005. His nomination was approved by the [Senate Judiciary Committee](http://en.wikipedia.org/wiki/Senate_Judiciary_Committee) in November 2005 but was never voted on by the full Senate, The Developing Legal Framework for Defensive and Offensive Cyber Operations, This speech was the Keynote address at the Harvard National Security Journal Symposium, <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf>

Congressional reporting. The National Security Act also ¶ requires the President and DNI to ensure that the Intelligence Committees ¶ of the House and Senate are fully and currently informed of all intelligence ¶ and counterintelligence activities, to the extent consistent with the ¶ protection of sensitive sources and methods or other exceptionally sensitive ¶ matters.10¶ With respect to covert actions, the Act requires the President to ¶ report presidential findings supporting covert actions to the Intelligence ¶ Committees, but where the President determines that it’s essential because ¶ of “extraordinary circumstances affecting vital interests of the United ¶ States,” the President may limit access to the so-called “Gang of Eight” —¶ the chairs and ranking members of the two Intelligence Committees, the ¶ Speaker and minority leader of the House, and the majority and minority ¶ leaders of the Senate, along with whatever other congressional leaders the ¶ President chooses to include.11¶ The **committee chairs hate when briefings are limited to the Gang of Eight, because they catch hell from the members** of their committees who ¶ are outside the circle. So when former-Senator Obama first became President, there was hope among some in Congress that he would eliminate the Gang of Eight briefings. But when Congress proposed an Intelligence ¶ Authorization bill that would do just that, President **Obama threatened to veto** it. Once he became head of the Executive Branch, he clearly ¶ understood the importance of being able to limit the scope of briefings for ¶ the most sensitive matters. So the statute still allows for Gang of Eight ¶ briefings In contrast to these title 50 intelligence activities, military operations conducted under title 10 authorities are subject to oversight by the Armed Services Committees of Congress. (Title 10 of the U.S. Code governs DoD’s ¶ military authorities and the military command structure; title 50 governs the ¶ Intelligence Community and intelligence activities.)¶ And make no mistake, in the world of Washington, it really does ¶ matter whether an activity is characterized as covert action or a traditional ¶ military action because different Executive Branch departments or agencies ¶ will have ownership of the operation and different committees of Congress ¶ will have oversight jurisdiction, and they all jealously guard their respective ¶ domains.

## Warfighting DA

#### Obama weak now- Syria deal

Maloof 9/13

F. Michael Maloof, senior staff writer for WND and the G2Bulletin, is a former security policy analyst in the Office of the Secretary of Defense¶ Read more at <http://www.wnd.com/2013/09/putin-makes-obama-look-indecisive-weak/#JFIueVqdjRHQa1GD.99> ETB

If Kerry and Lavrov come up with a plan, it will further consolidate Putin’s efforts in the Middle East, at U.S. expense.¶ “If the U.S. administration were to ignore Russian protests and proceed with a (military) strike with at least rhetorical coalition support, Russia would have little to show for its claimed influence in the Middle East,” according to the open intelligence group Stratfor.¶ “However, if Russia could effectively stunt the U.S.-led military campaign through an airy diplomatic proposal, then Russia will have played a hand in directly showcasing U.S. unreliability to its allies,” it said.¶ A proposal could make the U.S. look weak and indecisive while Moscow comes off “as the voice of reason” in a war that no one wants, and it will be all the Obama administration’s doing.

#### Obama is sending global signals of weakness and uncertainty

Forbes 9/1

<http://www.forbes.com/sites/dougschoen/2013/09/01/weak-on-syria-weak-in-the-world/> ETB

Put another way, the President made it clear a year ago that there was a red line that the Syrians should not cross. All evidence suggests that they have surely crossed it and instead of striking, the President lectures the American people, and indeed the world, on American democracy.¶ Indeed, just this morning, a Syrian state state-run newspaper called Obama’s decision to seek Congressional approval before taking military action “the start of the historic American retreat.” It doesn’t get clearer than that.¶ This is not a president who shies away from using his executive power. He has altered ObamaCare, pushed his gun control agenda to strengthen national background checks, delayed the deportation of illegal immigrants when Congress wouldn’t agree amongst many other examples. But he has now suddenly decided that before he takes action, action that is within his purview, he is going to seek Congressional approval that is almost impossible to predict as to whether it will be granted or not.¶ If Obama really wanted to go ahead he would have brought congress back into session immediately and not waited more than 10 days thereby giving the Syrians time to plan for an attack – should one ultimately come. And even then, Obama has made it clear any such attack will be limited in nature and scope and will not involve regime change.¶ It follows that the message Obama’s speech yesterday sends is a muddled one at best.¶ It said to the mullahs in Iran and their Supreme Leader Ali Khamenei that they can continue to pursue their nuclear program by enriching uranium and refining plutonium without having to fear that they will be precipitously attacked by the US.¶ And to Russia’s President Putin, who has been an unbendable ally of Assad, providing him with arms and anti-aircraft weaponry, Obama has shown that the balance of power in the Middle East has almost certainly shifted away from the US. This is all the more alarming as Putin said just yesterday that the idea that the Syrian regime used chemical weapons is “absolute nonsense.”¶ What’s more, with a totally incoherent American policy on Egypt wherein it is unclear who and what we support, the US’s approach to the Syria further paints a bleak picture of American power and potency. Indeed, with our only real achievement in the region being the recent appearance of convincing the Arabs and Israelis to come to the peace table, an image of American uncertainty is radiating across the globe.¶ And although this would be a serious accomplishment if progress is made, our inaction on Syria signals to Israel, one of our strongest allies, that we are not willing to stick our neck out for them, their safety and way of life.¶ To our allies around the world who have said that if we do not stand firm we will send the wrong message to the Syrians, Obama offered not much of a response other than to tell them, in so many words, that they may well have to go it alone.¶ The US has not been sending clear messages. And though it may be apparent to me that the President’s move was calculated to force responsibility on a reluctant Congress and to play to 80% of the American people who have said in polls that they are against intervention in Syria, that does not mean that the US is offering anything but a confused image of our mission in the world to both our allies and foes.¶ Thus, in the short term the President may have managed to escape from the political quandary he faces. But in the longer term, America looks weaker, feckless and more uncertain.¶ President Obama has, if nothing else, compounded the view of a weak leader heading an unsure nation. This is an image we can ill afford to project.

#### Massive alt causes to flex

Rozell 12

(Mark Rozell, Professor of Public Policy, George Mason University, “From Idealism to Power: The Presidency in the Age of Obama” 2012, <http://www.libertylawsite.org/book-review/from-idealism-to-power-the-presidency-in-the-age-of-obama/>, KB)

A substantial portion of Goldsmith’s book presents in detail his case that **various forces** outside of government, and some within, **are responsible for hamstringing the president** in unprecedented fashion: **Aggressive**, often intrusive, **journalism, that at times endangers national security; human rights and other advocacy groups**, some **domestic and** other **cross-national, teamed with big resources and talented, aggressive lawyers, using every legal category and technicality possible to complicate executive action**; **courts** thrust into the mix, **having to decide critical national security law controversies**,

even when the judges themselves have little direct knowledge or expertise on the topics brought before them; **attorneys within the executive branch** itself **advising against actions** based on often narrow legal interpretations and with little understanding of the broader implications of tying down the president with legalisms.

# 1AR

## Case

#### Prez will adhere to congressional constraints- fear of political costs

Bradley and Morrison ‘13

[Curtis A., William Van Alstyne Professor of Law, Duke Law School. Trevor W., Liviu Librescu Professor of Law, Columbia Law School. Columbia Law Review 113. <http://www.columbialawreview.org/wp-content/uploads/2013/05/Bradley-Morrison.pdf> ETB]

**In addition to the constraining influence arising from the internalization of legal norms** by executive branch lawyers and other officials, **law** ¶ **could constrain the President if there are “external” sanctions for** ¶ **violating it.** The core idea here is a familiar one, often associated with ¶ Holmes’s “bad man”139: One who obeys the law only because he ¶ concludes that the cost of noncompliance exceeds the benefits is still ¶ subject to legal constraint if the cost of noncompliance is affected by the ¶ legal status of the norm. This is true even though the law is likely to ¶ impose less of a constraint on such “bad men” than on those who have ¶ internalized legal norms, and even though it is likely to be difficult in ¶ practice to disentangle internal and external constraints. ¶ Importantly, **external sanctions for noncompliance need not be** ¶ **formal. If the existence or intensity of an informal sanction is affected by** ¶ **the legal status of the norm in question, compliance with the norm in** ¶ **order to avoid the sanction should be understood as an instance of law** ¶ **having a constraining effect**. **In the context of presidential compliance** ¶ **with the law, one can plausibly posit a number of such informal** ¶ **sanctions. One operates on the level of** professional **reputation,** and may ¶ be especially salient for lawyers in the executive branch. If a lawyer’s own ¶ internalization of the relevant set of legal norms is insufficient to prevent ¶ him from defending as lawful actions that he knows are obviously beyond ¶ the pale, he might respond differently if he believed his legal analysis ¶ would or could be disclosed to the broader legal community in a way that ¶ would threaten his reputation and professional prospects after he leaves ¶ government.140 (This concern might help further explain the OLC and other Justice Department officials’ resistance to the White House in the ¶ warrantless surveillance example discussed above.) ¶ Although **fear of harm to their professional reputations may indeed** ¶ **help constrain government lawyers**, if that were the only operative ¶ external sanction in this context it would be fair to ask whether it ¶ translated into a real constraint on the President in high-stakes contexts. ¶ But it is not the only potential sanction. **A** related and perhaps **more** ¶ **significant sanction may operate directly on political leaders within the** ¶ **government, including the President himself: partisan politics**. **If being** ¶ **perceived to act lawlessly is politically costly, a President’s political rivals** ¶ **will have an incentive to invoke the law to oppose him**. Put another way, ¶ **legal argumentation might have a salience with the media, the public at** ¶ **large, and influential elites that could provide presidential opponents in** ¶ **Congress and elsewhere with an incentive to criticize executive actions in** ¶ **legal terms. If such criticism gains traction in a given context, it could** ¶ **enable the President’s congressional opponents to impose even greater** ¶ **costs on him** through a variety of means, **ranging from oversight hearings** ¶ **to,** in the extreme case, threats of **impeachment**. Thus, **so long as the** ¶ **threat of such sanctions is credible, law will impose an external** ¶ **constraint**—whether or not the President himself or those responsible ¶ for carrying out his policies have internalized the law as a normative ¶ matter. **The prospect of political sanctions might help explain,** for ¶ example, **why modern Presidents do not seem to seriously contemplate** ¶ **disregarding Supreme Court decisions**.141 **And if Presidents are constrained to follow the practice-based norm of judicial supremacy, they** ¶ **may be constrained to follow other normative practices that do not** ¶ **involve the courts**. ¶ **Work by political scientists concerning the use of military force is at** ¶ **least suggestive of how a connection between public sanctions and law** ¶ **compliance might work**. As this work shows, **the opposition party in** ¶ **Congress, especially during times of divided government, will have both** ¶ **an incentive and the means to use the media to criticize unsuccessful** ¶ **presidential uses of force. The additional political costs that the** ¶ **opposition party is able to impose in this way will in turn make it less** ¶ **likely that Presidents will engage in large-scale military operations.1**42 It is ¶ at least conceivable, as the legal theorist Fred Schauer has suggested, that ¶ **the political cost of pursuing an ultimately unpopular policy initiative** ¶ (such as engaging in a war) **goes up with the perceived illegality of the initiative**.143 If that is correct, then **actors will require more assurance of** ¶ **policy success before potentially violating the law. This should count as a** ¶ **legal constraint on policymaking even if the relevant actors themselves** ¶ **do not see any normative significance in the legal rule in question.**