### 2AC T - Notification

#### It’s a check on presidential power

**Gaul 8**, Matthew J. Gaul is a partner in Steptoe’s New York office.  A former insurance regulator and securities enforcement attorney for the state of New York, Mr. Gaul represents insurance companies and other financial institutions in government investigations and complex regulatory matters, <http://faculty.lls.edu/manheim/ns/gaul2.htm>

The president may circumvent the specified waiting period by stating in his certification that a state of emergency exists which requires immediate approval of the exports.87 The emergency certification must also set forth "a detailed justification for his determination, including a description of the emergency circumstances which necessitate the immediate issuance of the export license and a discussion of the national security interests involved."88
The final **check on presidential regulatory power** in this area was added in 1996. The new provision requires the president to publish the above certifications in the federal register upon transmittal to the Speaker of the House and Chair of the Foreign Relations Committee.89 This public notification requirement only applies to major arms licenses for export deals totaling $50 million or more.

#### Restrict is to check free activity — they confuse it with restraint

**Oklahoma Attorney General**Opinions - 3/19/200**4**, Question Submitted by: The Honorable Mark Campbell, District Attorney, 19th District; The Honorable Jay Paul Gumm, State Senator, District 6, 2004 OK AG 7, [http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=43849](http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=438494" \t "_blank)

Accordingly, we must look to the plain and ordinary meaning of the term.*Webster's New International Dictionary*defines restrictions as follows: "something that restricts" and "a regulation that restricts or restrains." *Id.* at 1937 (3d ed. 1993). Restrict is defined as follows: "to set bounds or limits to: hold within bounds: as a : to check free activity, motion, progress, or departure." Id. Restrain is defined as to "prevent from doing something." *Id.* at 1936. Therefore, as used in Section 1125, "restrictions" is meant to describe those conditions of parole or probation which are intended to restrain or prevent certain conduct of the person subject thereto.

#### Congress is key to transparency

**Butler 4/26, Appellate Advocacy Counsel for the Electronic Privacy Information Center**, When Cyberweapons End Up On Private Networks: Third Amendment Implications for Cybersecurity Policy, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257078>

A. Authority: **Congress Must Be Involved in Establishing Any Framework for the Authorization of Cyberoperations** Given that the Third Amendment requires war-time quartering be conducted “in a manner to be prescribed by law,”223 Congress must have a role in establishing the framework used to authorize any offensive cyberoperation. This legislative involvement would not only ensure that all cyberoperations have adequate legal authorization but it would also promote the broader goals of transparency and cooperation that the President has emphasized throughout this process. So far Congress has focused its energy on perceived problems rather than real solutions.224 A debate raged in the 112th Congress over whether to let DHS or NSA take the lead on a proposed information-sharing environment.225 This turf war was quite tangential from the problems of substandard security for critical systems and a lack of legal clarity as to the role of each government agency in responding to an external threat or strategic opportunity.226 The only congressional involvement in developing a cybersecurity framework so far has been its brief affirmance in the 2012 National Defense Authorization Act227 that the President may conduct “operations in cyberspace” subject to the traditional legal regimes applicable to kinetic warfare.228 Congress’s active role in setting our nation’s military actions in cyberspace is the only way to have a national dialogue and to avoid relying on secret legal interpretations about important national security matters. The President took steps to begin a national dialogue when he issued an Executive Order on the same day as the 2013 State of the Union Address.229 The Executive Order focused on improving critical infrastructure cybersecurity while promoting privacy, civil liberties, and the economy.230 The Order also provided for sharing of “cyber threat information” from executive branch agencies to private sector entities,231 and the development of a framework by the National Institute of Standards and Technology (NIST) to establish baseline security standards for government agencies and critical infrastructure companies.232 The Order also required that privacy and civil liberties protections be incorporated into the cybersecurity program and that the Chief Privacy Officer of DHS assess the privacy risks and publish a report.233 The Executive Order did not address the “information sharing environment” proposed in Congress during 2012 and again in 2013.234 The Order also did not address the legal determination of when and how cyberoperations can be authorized, which has apparently already been made in an internal executive-branch memorandum.235 The President’s Executive Order is a step in the right direction but it **does not provide sufficient authority** for cyberoperations that could intrude upon civilian systems; **only Congress can authorize such quartering**.

#### Transparency’s key to Russian relations and developing global cybersecurity

**Ibrahim, Research Intern at CSIS, 13**, Karina G. Ibrahim is a research intern with the Russia and Eurasia Program at the Center for Strategic and International Studies and a recent graduate from the University of North Carolina at Chapel Hill. <http://csis.org/blog/arms-race-cyber-space-us-russian-relations-and-prospects-cyber-warfare>

In the month of June, the already strained U.S.-Russia relationship has once again been tested by developments in the cybersecurity field. Amidst cyber-attacks against the United States [purportedly emanating from Russia](http://en.rian.ru/russia/20130222/179615523.html) and the damaging revelations from U.S. former security contractor Edward Snowden, the two countries face difficulties in establishing cyber defense partnerships due to the legacy of mistrust and diverging national interests. However, U.S. cooperation with Russia[n advanced cyber actor](http://www.intelligence.senate.gov/130312/clapper.pdf), is **necessary to effectively manage cyber conflict**. Through the development of sustainable bilateral relations, U.S. and Russia can begin to invest in confidence-building and increase transparency to address the emergence of cybersecurity threats.

The failure of a U.S.-Russia cybersecurity partnership to develop stems from a history of mistrust, further exacerbated by the ongoing allegations of cyber-attacks and cyber-espionage (collectively referred to as cyberwarfare). [An increase in network probes and hacking attempts](http://www.intelligence.senate.gov/130312/clapper.pdf) suggests that Russia is either attempting to carry out cyber-intrusions against U.S. systems, or at least sanctioning such acts. Recently, [the Office of the National Counterintelligence Executive indicated](http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf) that “Russia’s intelligence services are conducting a range of activities to collect economic information and technology from U.S. targets.” However, the Russian government denies involvement in these alleged cyber-intrusions.

Similarly, recent developments in the Snowden case have undermined the potential for mutual cooperation. Snowden’s revelations about American cyber-espionage on its allies and other states have angered a number of European allies and raised questions about the goals of U.S. surveillance programs. These revelations, alongside Russia’s alleged offensive cyber activities, have reduced already low levels of trust between the U.S. and Russia and have stalled the development of a successful cyber defense initiative to mitigate global cybersecurity challenges.

#### Relations solve nuclear war

Allison & Blackwill 11, Fellow for Foreign Policy @ Council on Foreign Relations

[Graham, director of the Belfer Center for Science and International Affairs at Harvard’s Kennedy School, former assistant secretary of defense in the Clinton administration, Robert D., Henry A. Kissinger senior fellow for U.S. foreign policy -- Council on Foreign Relations, served as U.S. ambassador to India and as deputy national security adviser for strategic planning in the Bush administration, both co-chairmen of the Task Force on Russia and U.S. National Interests, co-sponsored by the Belfer Center and the Center for the National Interest, 10-30-11 Politico, “10 reasons why Russia still matters,” <http://dyn.politico.com/printstory.cfm?uuid=161EF282-72F9-4D48-8B9C-C5B3396CA0E6>]

That central point is that Russia matters a great deal to a U.S. government seeking to defend and advance its national interests. Prime Minister Vladimir Putin's decision to return next year as president makes it all the more critical for Washington to manage its relationship with Russia through coherent, realistic policies. No one denies that Russia is a dangerous, difficult, often disappointing state to do business with. We should not overlook its many human rights and legal failures. Nonetheless, Russia is a player whose choices affect our vital interests in nuclear security and energy. It is key to supplying 100,000 U.S. troops fighting in Afghanistan and preventing Iran from acquiring nuclear weapons. Ten realities require U.S. policymakers to advance our nation's interests by engaging and working with Moscow. First, Russia remains the **only nation that can erase the United States from the map in 30 minutes**. As every president since John F. Kennedy has recognized, Russia's cooperation is critical to averting nuclear war. Second, Russia is our most consequential partner in preventing nuclear terrorism. Through a combination of more than $11 billion in U.S. aid, provided through the Nunn-Lugar Cooperative Threat Reduction program, and impressive Russian professionalism, two decades after the collapse of the “evil empire,” not one nuclear weapon has been found loose. Third, Russia plays an essential role in preventing the proliferation of nuclear weapons and missile-delivery systems. As Washington seeks to stop Iran's drive toward nuclear weapons, Russian choices to sell or withhold sensitive technologies are the difference between failure and the possibility of success. Fourth, Russian support in sharing intelligence and cooperating in operations remains essential to the U.S. war to destroy Al Qaeda and combat other transnational terrorist groups. Fifth, Russia provides a vital supply line to 100,000 U.S. troops fighting in Afghanistan. As U.S. relations with Pakistan have deteriorated, the Russian lifeline has grown ever more important and now accounts for half all daily deliveries. Sixth, Russia is the world’s largest oil producer and second largest gas producer. Over the past decade, Russia has added more oil and gas exports to world energy markets than any other nation. Most major energy transport routes from Eurasia start in Russia or cross its nine time zones. As citizens of a country that imports two of every three of the 20 million barrels of oil that fuel U.S. cars daily, Americans feel Russia’s impact at our gas pumps. Seventh, Moscow is an important player in today’s international system. It is no accident that Russia is one of the five veto-wielding, permanent members of the U.N. Security Council, as well as a member of the G-8 and G-20. A Moscow more closely aligned with U.S. goals would be significant in the balance of power to shape an environment in which China can emerge as a global power without overturning the existing order. Eighth, Russia is the largest country on Earth by land area, abutting China on the East, Poland in the West and the United States across the Arctic. This territory provides transit corridors for supplies to global markets whose stability is vital to the U.S. economy. Ninth, Russia’s brainpower is reflected in the fact that it has won more Nobel Prizes for science than all of Asia, places first in most math competitions and dominates the world chess masters list. The only way U.S. astronauts can now travel to and from the International Space Station is to hitch a ride on Russian rockets. The co-founder of the most advanced digital company in the world, Google, is Russian-born Sergei Brin. Tenth, Russia’s potential as a spoiler is difficult to exaggerate. Consider what a Russian president intent on frustrating U.S. international objectives could do — from stopping the supply flow to Afghanistan to selling S-300 air defense missiles to Tehran to joining China in preventing U.N. Security Council resolutions. So next time you hear a policymaker dismissing Russia with rhetoric about “who cares?” ask them to identify nations that matter more to U.S. success, or failure, in advancing our national interests.

### Heg

### There’s no correlation between hegemony and stability

Fettweis, ’10

[Christopher J. Fettweis, Assistant Professor of Political Science at Tulane University, “Threat and Anxiety in US Foreign Policy,” Survival, 52:2, 59-82, March 25th 2010, <http://dx.doi.org/10.1080/00396331003764603>]

One potential explanation for the growth of global peace can be dismissed fairly quickly: US actions do not seem to have contributed much. The limited evidence suggests that there is little reason to believe in the stabilising power of the US hegemon, and that there is no relation between the relative level of American activism and international stability. During the 1990s, the United States cut back on its defence spending fairly substantially. By 1998, the United States was spending $100 billion less on defence in real terms than it had in 1990, a 25% reduction.29 To internationalists, defence hawks and other believers in hegemonic stability, this irresponsible ‘peace dividend’ endangered both national and global security. ‘No serious analyst of American military capabilities’, argued neo-conservatives William Kristol and Robert Kagan in 1996, ‘doubts that the defense budget has been cut much too far to meet America’s responsibilities to itself and to world peace’.30 And yet the verdict from the 1990s is fairly plain: the world grew more peaceful while the United States cut its forces. No state seemed to believe that its security was endangered by a less-capable US military, or at least none took any action that would suggest such a belief. No militaries were enhanced to address power vacuums; no security dilemmas drove insecurity or arms races; no regional balancing occurred once the stabilising presence of the US military was diminished. The rest of the world acted as if the threat of international war was not a pressing concern, despite the reduction in US military capabilities. Most of all, the United States was no less safe. The incidence and magnitude of global conflict declined while the United States cut its military spending under President Bill Clinton, and kept declining as the George W. Bush administration ramped the spending back up. Complex statistical analysis is unnecessary to reach the conclusion that world peace and US military expenditure are unrelated.

### 2AC Cyber Deterrence DA

#### No link — the plan is a notification requirement — Lorber says that doesn’t trigger the disad

#### 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.**

#### No link — the plan is just oversight, not a ban on OCOs — executive control makes deterrence unstable since other countries perceive irrationality when OCOs are controlled by one person — that’s Rothschild

#### 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 — norms make deterrence stable — only the plan solves — that’s CSM

#### 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 hesitation. 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.

### Econ

#### No link between the economy and war – history proves

Ferguson 6, Professor of History @ Harvard

(Ferguson, Niall. "The Next War of the World." Foreign Affairs 85.5 (Sept-Oct 2006): 61. Expanded Academic ASAP.)

There are many unsatisfactory explanations for why the twentieth century was so destructive. One is the assertion that the availability of more powerful weapons caused bloodier conflicts. But there is no correlation between the sophistication of military technology and the lethality of conflict. Some of the worst violence of the century -- the genocides in Cambodia in the 1970s and central Africa in the 1990s, for instance -- was perpetrated with the crudest of weapons: rifles, axes, machetes, and knives. Nor can economic crises explain the bloodshed. What may be the most familiar causal chain in modern historiography links the Great Depression to the rise of fascism and the outbreak of World War II. But that simple story leaves too much out. Nazi Germany started the war in Europe only after its economy had recovered. Not all the countries affected by the Great Depression were taken over by fascist regimes, nor did all such regimes start wars of aggression. In fact, no general relationship between economics and conflict is discernible for the century as a whole. Some wars came after periods of growth, others were the causes rather than the consequences of economic catastrophe, and some severe economic crises were not followed by wars.

### 2AC Politics DA

#### Obama already spent capital on Syria and it was perceived as a loss

Bohan, 9/11 (Caren, 9/11/2013, “Delay in Syria vote frees Obama to shift to hefty domestic agenda,” <http://www.reuters.com/article/2013/09/11/usa-obama-agenda-idUSL2N0H716N20130911>))

WASHINGTON, Sept 11 (Reuters) - Putting off a decision on military strikes on Syria allows President Barack Obama to shift his attention back to a weighty domestic agenda for the fall that includes budget fights, immigration and selecting a new chairman of the Federal Reserve.

Obama and his aides have immersed themselves for a week and a half in an intensive effort to win support in Congress for U.S. military action in Syria after a suspected chemical weapons attack last month killed more than 1,400 people.

But the effort, which included meetings by Obama on Capitol Hill on Tuesday followed by his televised speech to Americans, seemed headed for an embarrassing defeat, with large numbers of both Democrats and Republicans expressing opposition.

The push for a vote on Syria - which has now been delayed - had threatened to crowd out the busy legislative agenda for the final three months of 2013 and drain Obama's political clout, making it harder for him to press his priorities.

But analysts said a proposal floated by Russia, which the Obama administration is now exploring, to place Syria's weapons under international control may allow Obama to emerge from a difficult dilemma with minimal political damage.

"He dodges a tough political situation this way," said John Pitney, professor of politics at Claremont McKenna College in California.

Pitney said the delay in the Syria vote removes a big burden for Obama, given that Americans, who overwhelmingly opposed military intervention in Syria, will now be able to shift their attention to other matters.

He said Obama could suffer some weakening of his leverage with Congress. The administration's "full court press" to try to persuade lawmakers to approve military force on Syria was heavily criticized and did not yield much success.

"He probably has suffered some damage in Congress because there are probably many people on (Capitol Hill) who have increasing doubts about the basic competence of the administration and that's a disadvantage in any kind of negotiation," Pitney said.

#### Immigration push makes the link inevitable

Hughes, 9/11 --- White House Correspondent at Washington Examiner (Brian, 9/11/2013, “Syria push imperils Obama's fall agenda,” [http://washingtonexaminer.com/syria-push-imperils-obamas-fall-agenda/article/2535611)](http://washingtonexaminer.com/syria-push-imperils-obamas-fall-agenda/article/2535611%29))

Obama will also face a difficult challenge reviving immigration reform, which stalled in the GOP-controlled House after senators approved a bipartisan bill. In his State of the Union address, Obama said immigration reform would be a key priority of his second term.

#### 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).

#### It’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.

### 2AC PC Defense

#### Debt ceiling will inevitably be increased

Sahadi, 9/12 (Jeanne, “The never-ending charade of debt ceiling fights,” <http://money.cnn.com/2013/09/12/news/economy/debt-ceiling/?source=cnn_bin)>)

Lawmakers are tied up in knots over increasing the debt ceiling this fall. But they eventually will. The only question is how messy the process will be.

Why assume they'll raise it? Because they have no real choice if they want to avoid a U.S. default. A default would hurt the economy and markets, and most lawmakers know this. That's why they regularly raise the debt ceiling before it comes to that.

In fact, since 1940, Congress has effectively approved 79 increases to the debt ceiling. That's an average of more than one a year.

How do they raise it? Sometimes lawmakers have raised it by small amounts, other times by large amounts. And sometimes they've raised it "temporarily" with provisions for a "snap-back" to a lower level.

Since it's a politically tough vote, they occasionally devise clever ways to tacitly approve increases without ever having to publicly record a "yes" vote.

For example, as part of the deal to resolve the 2011 debt ceiling war, Congress approved a plan that let President Obama raise the debt limit three times unless both the House and Senate passed a "joint resolution of disapproval." Such a measure never materialized. And even if it had, the president could have vetoed it.

Then this past February, lawmakers decided to temporarily "suspend" the debt ceiling.

Under this scheme, Treasury was able to continue borrowing to pay the country's bills until May 19. At that point, the debt limit automatically reset to the old cap plus whatever Treasury borrowed during the suspension period.

Related: Debt ceiling 'X' date could hit Oct. 18

What does raising the debt ceiling accomplish? Despite some politicians' incorrect assertions, raising the debt ceiling does not give the government a "license to spend more."

It simply lets Treasury borrow the money it needs to pay all U.S. bills in full and on time. Those bills are for services already performed and entitlement benefits already approved by Congress. In other words, it's a license to pay the bills the country incurs as a result of past decisions made by lawmakers from both parties over the years.

Refusing to raise the debt ceiling is "not like cutting up your credit cards. It's like cutting up your credit card bills," said historian Joseph Thorndike, who has written about past debt crises.

How high is it today? The debt ceiling was reset at $16.699 trillion on May 19, up from the $16.394 trillion where it was before the suspension.

Since then, Treasury has been forced to use "extraordinary measures" to keep the country from breaching the limit.

Treasury Secretary Jack Lew said those measures will be exhausted by mid-October, after which he will only have $50 billion on hand, plus incoming revenue to pay what's owed. Sounds like a lot, but it won't last long.

How long will it last? An analysis by the Bipartisan Policy Center estimates that the Treasury will no longer be able to pay all bills in full and on time at some point between Oct. 18 and Nov. 5.

So, you're saying they only have a few weeks to work this out? Yup.

House Republicans say they will demand spending cuts and fiscal reforms in exchange for their support of a debt ceiling increase. The White House, meanwhile, has said it won't negotiate quid pro quos.

The question is when will Republicans or the White House -- or both - bend in the standoff? If recent history is any guide it likely will be just in the nick of time.

And there's no telling how creative the deal they cut will be.

But any bad blood created along the way almost certainly would poison other budget negotiations. To top of page

### 1AR

#### There will be South China Sea war - China’s expansion to South China Sea is rooted in historical national identity

**Prabhakar 11** Dr.W.Lawrence S., Associate Professor, Department of Political Science, Madras Christian College, Chennai, India; Adjunct Senior Fellow, Centre for Asian Strategic Studies, New Delhi, India; Guest Professor, Department of Humanities and Social Sciences, Indian Institute of Technology-Madras., “ The Evolving Geopolitics in the South China Sea”, PDF

Sovereignty Concerns and the apprehension of sovereignty violations by contending states both regional and extra-regional is a dominant factor in the region. Sovereignty concerns are derivative of the historical and colonial factors that have shaped the national identities and resistance to external domination. Territorial and maritime disputes and contentions over unresolved border and boundary issues have been emerged as vital points of assertion of national sovereignty. Regional responses to territorial disputes have been in the form of modernization of naval forces and air forces that are viewed as viable instruments to secure the islands and protect the maritime areas **The South China Sea is yet another source of national identity for China.** The “recovery” of the area for the Chinese leaders provides a means to erase a century of national humiliation of colonialism and “unjust treaties” that China was subjected to. **China views the issue as a part of the domestic issue** and hence the Law of the People’s Republic of China on the Territorial Waters and Contiguous Areas was passed by the National People’s Assembly as a means to recover the area to Chinese suzerainty. China reiterated claims in the South China Sea and stipulated the right to use force to protect islands-- the Spratlys and their surrounding waters. The law questioned the peaceful management of the territorial dispute and was regarded by the Association as a political provocation. **The PLA tends to view the South China Sea as a domestic issue-- a derivative of China’s national identity.** Superimposed on the patterns of power rivalry from the ancient period that had witnessed several power transitions between China, Japan, Korea and India, thus **the South China Sea** and the East China Sea **have been flash points that have intermittently triggered in different periods of history**. With the Cold war overlay since 1945-1991, the region was relatively calm thanks to the large measure of the strategic balancing of the United States and the Soviet Union—although the Cold war had witnessed the worst Indo-China conflict that raged for several years. In the post-cold war period and into the midway of the Globalization period, the South China Sea had emerged as vital hub for contending maritime access between China and most of the Southeast Asian states of Malaysia, Singapore, Vietnam, Philippines, Taiwan, Brunei, Thailand, Cambodia with most of the contentions over Spratlys and Paracels archipelago besides the other islands with contenders like the Woody Island (China) Layang Layang (Malaysia), Truong Sa Lon(Vietnam), Taipingdao (Taiwan), Pagasa (Rancudo) Airfield) (Philippines). These islands offer mid-sea access that could serve for amphibious and aerial staging points in a sea of contending territorial and resources disputes.