# 1AC

**1AC — Plan Text**

**The legislative branch of the United States Federal Government should prohibit the use of offensive cyber operations about which Congress has not been notified.**

**1AC — Cyber War**

**Contention one is Cyber War:**

**The cyber arms race is accelerating — major attacks are inevitable this year — the best data proves**

**Goldman 13**, CNN Writer, Nations Prepare for Cyberwar, <http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html>

Security analysts are predicting that **2013 is when nation-sponsored cyberwarfare goes mainstream** -- and some think such attacks will lead to actual deaths.

In 2012, [large-scale cyberattacks targeted at the Iranian government](http://money.cnn.com/2012/05/30/technology/flame-virus/index.htm?iid=EL) were uncovered, and in return, Iran is believed to have launched [massive attacks aimed at U.S. banks](http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html?iid=EL) and Saudi oil companies. At least **12 of the world's 15 largest military powers are currently building cyberwarfare programs**, according to James Lewis, a cybersecurity expert at the **C**enter for **S**trategic and **I**nternational **S**tudies.

So a [cyber Cold War](http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm?iid=EL) is already in progress. But some security companies believe that battle will become even more heated this year.

"Nation states and armies will be more frequent actors and victims of cyberthreats," a team of researchers at McAfee Labs, an Intel ([INTC](http://money.cnn.com/quote/quote.html?symb=INTC&source=story_quote_link), [Fortune 500](http://money.cnn.com/magazines/fortune/fortune500/2012/snapshots/642.html?iid=EL))subsidiary, wrote in a[recent report](http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf).

Michael Sutton, head of security research at cloud security company [Zscaler](http://www.zscaler.com/), said he expects governments to spend furiously on building up their cyber arsenals. Some may even outsource attacks to online hackers.

The Obama administration and many in Congress have been[more vocal](http://money.cnn.com/2012/04/27/technology/cispa-cybersecurity/index.htm?iid=EL) about how an enemy nation or a terrorist cell could target the country's critical infrastructure in a cyberattack. Banks, stock exchanges, nuclear power plants and water purification systems are particularly vulnerable, **according to numerous assessments** delivered to Congress last year.

**And, cyber arms race causes world war — there are no checks on escalation, deterrence doesn’t apply, and only a certain commitment to the plan solves**

**CSM 11**, Christian Science Monitor

(3/7, Mark Clayton, The new cyber arms race, www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race)

**The new cyber arms race** Tomorrow's wars will be fought not just with guns, but with the click of a mouse half a world away that will unleash weaponized software that could take out everything from the power grid to a chemical plant. Deep inside a glass-and-concrete office building in suburban Washington, Sean McGurk grasps the handle of a vault door, clicks in a secret entry code, and swings the steel slab open. Stepping over the raised lip of a submarinelike bulkhead, he enters a room bristling with some of the most sophisticated technology in the United States. Banks of computers, hard drives humming on desktops, are tied into an electronic filtering system that monitors billions of bits of information flowing into dozens of federal agencies each second. At any given moment, an analyst can pop up information on a wall of five massive television screens that almost makes this feel like Cowboys Stadium in Arlington, Texas, rather than a bland office building in Arlington, Va. The overriding purpose of all of it: to help prevent what **could lead to the next world war**. Specifically, the "Einstein II" system, as it is called, is intended to detect a large cyberattack against the US. The first signs of such an "electronic Pearl Harbor" might include a power failure across a vast portion of the nation's electric grid. It might be the crash of a vital military computer network. It could be a sudden poison gas release at a chemical plant or an explosion at an oil refinery. Whatever it is, the scores of analysts staffing this new multimillion-dollar "watch and warn" center would, presumably, be able to see it and respond, says Mr. McGurk, the facility director. The National Cybersecurity and Communications Integration Center (NCCIC, pronounced en-kick) is one of the crown jewels of the Department of Homeland Security (DHS). It is linked to four other key watch centers run by the FBI, the Department of Defense (DOD), and the National Security Agency (NSA) that monitor military and overseas computer networks. **They are** monuments to what is **rapidly becoming a new global arms race.** **In the future, wars will** not just be fought by soldiers with guns or with planes that drop bombs. They will also **be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs** that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships. "The next time we want to go to war, maybe we wouldn't even need to bomb a country," says Liam O'Murchu, manager of operations for Symantec Security Response, a Mountain View, Calif., computer security firm. "We could just, you know, turn off its power." In this detached new warfare, soldiers wouldn't be killing other soldiers on the field of battle. But it doesn't mean there might not be casualties. Knocking out the power alone in a large section of the US could sow chaos. What if there were no heat in New England in January? No refrigeration for food? The leak of a radiation plume or chemical gas in an urban area? A sudden malfunction of the stock market? A disrupted air traffic control system? These are the darkest scenarios, of course – the kind that people spin to sell books and pump up budgets for new cyberwar technology. Interviews with dozens of cyberconflict experts indicate that this kind of strategic, large-scale digital warfare – while possible – is not the most likely to happen. Instead, some see a prolonged period of aggressive cyberespionage, sabotage, and low-level attacks that damage electronic networks. As one recent study done for the Organization for Economic Cooperation and Development put it: "It is unlikely that there will ever be a true cyberwar." Yet others say that conclusion might be too conservative. The fact is, no one knows for sure where digital weaponry is heading. **The cyber arms race is still in its infancy, and once a cybershot is fired, it's hard to predict where the fusillade might end**. In the seconds or minutes it might take staffers at the NCCIC to detect an attack, it could have already spread to US water supplies, railway networks, and other vital industries. How does the US military respond – or even know whom to retaliate against? If it does hit back, how does it prevent cyberweapons from spreading damage electronically to other nations around the world? Policy experts are just beginning to ask some of these questions as the cyberweapons buildup begins. And make no mistake, it is beginning. By one estimate, more than 100 nations are now amassing cybermilitary capabilities. This doesn't just mean erecting electronic defenses. It also means developing "offensive" weapons. Shrouded in secrecy, the development of these weaponized new software programs is being done outside public view and with little debate about their impact on existing international treaties and on conventional theories of war, like deterrence, that have governed nations for decades. "**Here's the problem – it's 1946 in cyber**," says James Mulvenon, a founding member of the Cyber Conflict Studies Association, a nonprofit group in Washington. "So **we have these potent new weapons, but we don't have all the conceptual and doctrinal thinking that supports those weapons or any kind of deterrence**. Worse, it's not just the US and Soviets that have the weapons – it's millions and millions of people around the world that have these weapons." In the new cyber world order, the conventional big powers won't be the only ones carrying the cannons. Virtually any nation – or terrorist group or activist organization – with enough money and technical know-how will be able to develop or purchase software programs that could disrupt distant computer networks. And the US, because it's so wired, is more vulnerable than most big powers to this new form of warfare. It's the price the country may one day pay for being an advanced and open society. "If the nation went to war today, in a cyberwar, we would lose," Mike McConnell, director of national intelligence from 2007 to 2009, told a US Senate committee a year ago. "We're the most vulnerable. We're the most connected. We have the most to lose." Still, none of this means people should immediately run for a digital fallout shelter. Many analysts think the cyberwar threat is overblown, and the US is developing sophisticated defenses, such as the digital ramparts here in Arlington. The question is: Will it be enough, or will it all amount to a Maginot line? ALAMOGORDO REDUX The cyber equivalent of the dropping of the atom bomb on Hiroshima came last fall. That's when the world found out about Stuxnet, the software program that wasn't just another annoying virus. It was a sophisticated digital superweapon. Unlike typical malicious software – Trojans and viruses that lurk hidden in a computer to, say, steal a bank account password or some proprietary corporate information – Stuxnet was designed to inflict damage in the real world. In this case it was apparently intended to destroy machines critical to Iran's nuclear ambitions. The marauding software was introduced into Iranian computers in five locations sometime in 2009, probably, experts believe, by an infected "thumb drive," a portable memory stick, inserted into the network by unwitting Russian engineers who were working on the Iranian nuclear facility. Once inside the system, analysts say, Stuxnet sought out its target, the computer-controlled nuclear centrifuge system, and sabotaged the machinery. Experts believe, in the end, the software may have damaged up to 1,000 of the plant's centrifuges. It did so without any human help – without anyone clicking a mouse or guiding it electronically. Since its emergence, Stuxnet has demonstrated that cyberattacks will not remain just banal attempts to delete or steal information inside computers or on the Internet. It showed that a cyberweapon can destroy actual plants and equipment – strategically important equipment. It is a "game changer," McGurk told Congress last fall. Experts believe that Stuxnet was developed by a nation with a top-notch covert cyberweapons team, probably at a cost of millions of dollars. But now that elements of its software code – its electronic blueprint – are available on the Internet, it could be downloaded and reverse-engineered by organized crime groups, cyberweapons dealers, so-called "hactivist" organizations, rogue nations, and terrorists. The hactivist group Anonymous recently touted that it had acquired a copy of the Stuxnet code. Individual tinkerers are getting it, too. "What Stuxnet represents is a future in which people with the funds will be able to buy a sophisticated attack like this on the black market," says Ralph Langner, a German cyber-security researcher and Stuxnet expert. "Everyone can have their own cyberweapon." He adds that Stuxnet could be modified by someone who isn't even a control-systems expert into a "digital dirty bomb" that could damage or destroy virtually any industrial operating system it targets. Amr Thabet, an engineering student at the University of Alexandria in Egypt, typifies how easy it is to access the new world of cyberweaponry. During recent mass street protests in his country, he found time to post on his blog a portion of the Stuxnet cyberweapon he had reverse-engineered. The blog drew the attention of cybersecurity experts, who were unhappy, but not surprised, by what he had done. "This kid's work makes Stuxnet a lot more accessible and portable to other computer architectures," says Bob Radvanovsky, an industrial control-systems expert at Infracritical, a Chicago-based computer security organization. "It's something a number of people are doing for intellectual exercise – or for malicious purposes. It's not a good trend. If a college student is trying to dabble with this, who else on the dark nets with more nefarious intentions might be [as well]? In an e-mail interview, Mr. Thabet said he did it largely for the thrill. He noted that he spent two months deconstructing a small but crucial part of the code after he saw all the attention surrounding the discovery of Stuxnet last fall. "It's the first time I see a malware becomes like a gun or like a weapon close a whole company in few days," he writes in broken English. "You can say [Stuxnet] makes the malware a harder challenge and more dangerous. That's maybe what inspire me." THE 'WAR' HAS ... ALREADY BEGUN? Definitions of what constitute a "cyberattack" or "cyberwar" vary, but experts roughly agree the US is now immersed in a continuous series of cyberconflicts. These are with state and nonstate actors, from Russia and China to criminal gangs and online protest groups. "Are we in a cyberwar now?" asks John Bumgarner, research director at the US Cyber Consequences Unit, a Washington-based think tank, who once was a cyberwarrior with the US Army. "No, not yet. Are we being targeted and our nation's networks attacked and infiltrated by nations that may be our adversaries in the future? Yes." Melissa Hathaway, former acting senior director for cyberspace at the National Security Council, says the threat is less a military one by nation-states and more about the need to protect US intellectual property from spies and organized crime groups. "We are currently in an economic cyberwar," Ms. Hathaway says. "It is costing our corporations their innovation, costing Americans their jobs, and making us a country economically weaker over the long term. I don't see it emerging as a military conflict, but as an economic war in which malware and our own digital infrastructure is being used to steal our future." Others agree that a strategic cyberwar isn't likely right now. But they do see the potential for escalation beyond the theft of the latest blueprints for an electric car or jet-fighter engine, particularly as the technology of digital warfare advances and becomes a more strategic imperative. "We in the US tend to think of war and peace as an on-off toggle switch – either at full-scale war or enjoying peace," says Joel Brenner, former head of counterintelligence under the US Director of National Intelligence. "The reality is different. We are now in a constant state of conflict among nations that rarely gets to open warfare.... What we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyberconflict with us." While he agrees the notion of big-scale cyberwarfare has been over-hyped, he says attacks that move beyond aggressive espionage to strikes at, or sabotage of, industrial processes and military systems "will become a routine reality." ANYTHING YOU CAN DO, WE CAN DO BETTER The attacks were coordinated but relatively unsophisticated: In the spring of 2007, hackers blocked the websites of the Estonian government and clogged the country's Internet network. At one point, bank cards were immobilized. Later, in 2008, similar cyberstrikes preceded the Russian invasion of Georgia. Moscow denied any involvement in the attacks, but Estonia, among others, suspected Russia. Whoever it was may not be as important as what it's done: touched off a mini cyber arms race, accelerated by the Stuxnet revelation. Germany and Britain announced new cybermilitary programs in January. In December, Estonia and Iran unveiled cybermilitias to help defend against digital attack. They join at least 20 nations that now have advanced cyberwar programs, according to McAfee, a Santa Clara, Calif., computer security firm. Yet **more than 100 countries have at least some cyberconflict prowess, and multiple nations "have the capability to conduct sustained, high-end cyberattacks** against the US," according to a new report by the Cyber Conflict Studies Association. McAfee identifies a handful of countries moving from a defensive to a more offensive posture – including the US, China, Russia, France, and Israel. Experts like Mr. Langner say the US is the world's cyber superpower, with weapons believed to be able to debilitate or destroy targeted computer networks and industrial plants and equipment linked to them. Indeed, China widely assumes that their nation's computer systems have been "thoroughly compromised" by the US, according to Dr. Mulvenon of the Cyber Conflict Studies Association, even as the Chinese penetrate deeper into US industrial and military networks. As well armed as the US is, however, its defenses are porous. The US may have the mightiest military in the world, but it is also the most computerized – everything from smart bombs to avionics to warship controls – making it unusually vulnerable to cyberassault. The DOD's communication system includes some 15,000 computer networks and 7 million computing devices. According to the Pentagon, unknown attackers try to breach its systems 6 million times a day. More than a few attempts have succeeded. Hackers are believed to have stolen key elements of the F-35 jet fighter a few years ago from a defense contractor. In 2008, infiltrators used thumb drives to infect the DOD's classified electronic network, resulting in what Deputy Defense Secretary William Lynn later called the "most significant breach of US military computers ever." Unlike many of its potential adversaries, the Pentagon is heavily reliant on computer networks. Over the past two decades, US industry, along with the military and federal agencies, have linked some networks and elements of the nation's infrastructure – power plants, air traffic control systems, rail lines – to the notoriously insecure Internet. It makes it easier, faster, and cheaper to communicate and conduct business – but at a cost. Almost all electrical power used by US military bases, for instance, comes from commercial utilities, and the power grid is a key target of adversaries. "We're pretty vulnerable today," says a former US national security official. "Our defense is superporous against anything sophisticated." Countries that are less wired are less vulnerable, which represents another danger. Some analysts even suggest that a small power like North Korea could do serious damage to the US in a cyberattack while sustaining relatively little itself. In a report presented at a NATO conference, former NSA expert Charlie Miller estimated that Pyongyang would need only about 600 cyber experts, three years, and $50 million to overtake and defeat America in a digital war. "One of North Korea's biggest advantages is that it has hardly any Internet-connected infrastructure to target," he says. "On the other hand, the US has tons of vulnerabilities a country like North Korea could exploit." The elite group of hackers sit at an oval bank of computers in a second-floor office on the wind-swept plains of Idaho. Their mission: infiltrate the computer network of Acme Products, an American industrial plant. They immediately begin probing for ways around the company's cyberdefenses and fire walls. Within minutes, they tap into the plant's electronic controls, sabotaging the manufacturing process. "They're already inside our system," howls an Acme worker, looking at his unresponsive computer after only 20 minutes. "They've got control of the lights. We can't even control our own lights!" Less than a half-hour later, a plastic vat is overflowing, spraying liquid into an industrial sink. The company's attempts to retake control of the system prove futile. Is the leak a toxic chemical? Something radioactive? Fortunately, in this case it is water, and the company itself is fictitious. This is simply an exercise by members of the DHS's Industrial Control System-Computer Emergency Readiness Team (ICS-CERT), simulating an attack and defense of a company. The message to emerge from the war game is unmistakably clear: Industrial America isn't well prepared for the new era of cyberwar, either. "We conduct these training classes to alert industry to what's really going on and educate them as to vulnerabilities they may not have thought of," says a senior manager at the Idaho National Laboratory (INL) in Idaho Falls, where the readiness team is located. Down the street, in another warehouselike building, high walls and locked doors shroud rooms where commercial vendors bring their industrial-control software to be probed for weaknesses by the cyber teams. Despite all the efforts here, experts say gaping holes exist in America's commercial electronic defenses. One reason is the vast number of people and organizations trying to penetrate the networks of key industries. Some people liken the intensity of the spying to the height of the postwar rivalry between the US and the Soviet Union – only the snooping now isn't just by a few countries. "I personally believe we're in the middle of a kind of cyber cold war," says a senior industrial control systems security expert at INL. "Over the past year our team has visited 30 to 40 companies in critical infrastructure industries – looking for threats on their [networks and industrial-control] systems – to see the level of penetration. In every case, teams of professionals were already there, embedded on every system." If only part of this infiltration turned out to be corporate espionage, that would be bad enough. But there's a more insidious threat lurking underneath. In his book "Cyber War," Richard Clarke, former counterterrorism chief with the National Security Council, writes that foreign nations are "preparing the battlefield" in key US industries and military networks, in part by creating "trapdoors" in electronic industrial-control systems. These trapdoors, in the form of nearly invisible software "rootkits," are designed to give the attacker access and control over industries' computer networks, which could later be used to disrupt or destroy operations – for instance, of the US power grid. "These hackers are invading the grid's control systems right now where it's easiest, getting themselves in position where they could control things if they wanted to," says the senior cybersecurity expert. "But they're not controlling them yet." Michael Assante, a former Navy cyberwarfare specialist and INL industrial-security expert, sees calculated hacking taking place as well. "I agree we have a lot of cyberespionage going on and a lot of preparation of the battlefield," he says in an interview at his home on a butte overlooking Idaho's Snake River Valley. "There's no question the grid is vulnerable." THE GENIE IS OUT OF THE HARD DRIVE Despite their dangers, cyberweapons hold clear appeal to the US and other nations. For one thing, they don't involve shooting people or inflicting casualties in a conventional sense. If fewer people die from bombs and bullets as a result of surreptitious software programs, nations may be more inclined to use them to try to deal with intractable problems. Cyberweapons may also be far cheaper than many conventional weapons. No doubt these are among the reasons President Obama has accelerated the development of US cybersecurity efforts, building on programs begun late in the tenure of President George W. Bush. In 2009, when announcing the new position of cybersecurity coordinator, Mr. Obama called digital infrastructure a "strategic national asset." Then, last spring, the Pentagon unveiled its joint US Cyber Command to accelerate and consolidate its digital warfare capabilities – including the ability to strike preemptively. Cyberspace was added to sea, air, land, and space as the fifth domain in which the US seeks "dominance." "Given the dominance of offense in cyberspace, US defenses need to be dynamic," wrote Mr. Lynn in Foreign Affairs magazine. "Milliseconds can make a difference, so the US military must respond to attacks as they happen or even before they arrive." Yet **the digital war buildup could have far-reaching – and unexpected – consequences. Cyberweapons are hardly clinical or benign**. They can infect systems globally in minutes that were not the intended target. Experts say Stuxnet, a self-propagating "worm," corrupted more than 100,000 Windows-based computers worldwide. Its damage could have been far more widespread if the digital warhead had been written to activate on any industrial-control system it found instead of just the one it targeted in Iran. **Because strikes and counterstrikes can happen in seconds, conflicts could quickly escalate outside the world of computers**. What, for instance, would the US do if an adversary knocked out a power plant – would it retaliate with digital soldiers or real ones? NATO and other organizations are already weighing whether to respond militarily against nations that launch or host cyberattacks against member states. "**The US cybersecurity strategy** since 2003 **has stated that we're not just going to respond to cyberattacks with cyber,**" says Greg Rattray, a former director of cybersecurity for the National Security Council. "If somebody cripples the US electric grid, a nuclear power plant, or starts to kill people with cyberattacks, **we have reserved the right to retaliate by the means we deem appropriate**." **Yet figuring out whom to retaliate against is far more complicated in a cyberwar than a conventional war. It's not just a matter of seeing who dropped the bombs. The Internet and the foggy world of cyberspace provide ample opportunity for anonymity.** The US and other countries are working on technical systems that would allow them to reverse-engineer attacks, detecting identifying elements among tiny packets of information that bounce among servers worldwide. Yet even if cybersleuths can trace the source of a strike to an individual computer, it might be located in the US. Foreign governments could send elite hackers into other countries to infiltrate networks, making it harder to follow the electronic trail. "Access is the key thing," says Dr. Brenner, the former counterintelligence chief. "If we ever get to real hostilities, all these attacks are going to be launched from within the US...." **All this makes it difficult to apply conventional doctrines of war, such as deterrence** and first-strike capability, **to the new era of cyberconflict. Does the US retaliate if it's unsure of who the enemy is? Can there be deterrence if retaliation is uncertain**? There are more mundane questions, too: When does aggressive espionage cross a threshold and constitute an "attack"? "**We live in a glass house so we better be careful about throwing rocks," says Hathaway of America's presumed prowess in offensive cyberwar and espionage tactics. "We don't have the resilience built into our infrastructure today to enter into such an escalated environment." In the face of such ambiguity**, many experts say **the US needs an overarching policy that governs the use of cyberweapons**. On the plus side, multiple cyberattack technologies "greatly expand the range of options available to US policy makers as well as the policy makers of other nations...," the National Academy of Sciences concluded in a landmark 2009 study. On the other hand, **"today's policy and legal framework for guiding and regulating the US use of cyberattack is ill-formed, undeveloped, and highly uncertain.**”

**That culminates in 3 scenarios for nuclear war**

**Austin, 8/6, Director of Policy Innovation at the EastWest Institute**, Costs of American Cyber Superiority, <http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/>

The United States is racing for the technological frontier in military and intelligence uses of cyber space. It is ahead of all others, and has mobilized massive non-military assets and private contractors in that effort. This constellation of private sector opportunity and deliberate government policy has been aptly labeled in recent months and years by so many credible observers (in The Economist, The Financial Times and the MIT Technology Review) as the cyber industrial complex.

The United States is now in the unusual situation where the head of a spy agency (NSA) also runs a major military unified command (Cyber Command). This is probably an unprecedented alignment of Praetorian political power in any major democracy in modern political history. This allocation of such political weight to one military commander is of course for the United States to decide and is a legitimate course of action. But it has consequences. The Snowden case hints at some of the blow-back effects now visible in public. But there are others, less visible.

The NSA Prism program exists because it is technologically possible and there have been no effective restraints on its international targeting. This lack of restraint is especially important because the command and control of strategic nuclear weapons is a potential target both of cyber espionage and offensive cyber operations. The argument here is not to suggest a similarity between the weapons themselves, but to identify correctly the very close relationship between cyber operations and nuclear weapons planning. Thus the lack of restraint in cyber weapons might arguably affect (destabilize) pre-existing agreements that **constrain nuclear weapons deployment and** possible **use**.

The cyber superiority of the United States, while legal and understandable, is now a cause of strategic instability between nuclear armed powers. This is similar to the situation that persisted with nuclear weapons themselves until 1969 when the USSR first proposed an end of the race for the technological frontier of potential planetary devastation. After achieving initial capability, the U.S. nuclear missile build up was not a rational military response to each step increase in Soviet military capability. It was a race for the technological frontier – by both sides – with insufficient recognition of the consequences. This conclusion was borne out by a remarkable Top Secret study commissioned in 1974 by the U.S. Secretary of Defense, Dr James Schlesinger. By the time it was completed and submitted in 1981, it assessed that the nuclear arms build-up by both sides was driven – not by a supposed tit for tat escalation in capability of deployed military systems – but rather by an unconstrained race for the technological limits of each side’s military potential and by its own military doctrinal preferences. The decisions of each side were not for the most part, according to this now declassified study, a direct response to particular systems that the other side was building.

**And low response times means there’s a greater timeframe and probability than traditional nuclear escalation**

**Dycus, Professor of National Security Law, 10**, Stephen is a Professor of national security law at Vermont Law School, former member of the National Academies committee on cyber warfare, LLM, Harvard University, LLB, BA, Southern Methodist University, “Congress’ Role in Cyber Warfare,” Journal of National Security Law & Policy, 4(1), 2010, p.161-164, <http://www.jnslp.com/read/vol4no1/11_Dycus.pdf>

In other ways, cyber weapons are **critically different from their nuclear counterparts**. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.

**The mere perception of Presidential control of OCOs fuels foreign uncertainty that causes extinction**

**Rothschild 2/13**, Editor of Progressive Magazine, Matthew Rothschild is the editor of The Progressive magazine, which is one of the leading voices for peace and social justice in this country. Rothschild has appeared on Nightline, C-SPAN, The O'Reilly Factor, and NPR, and his newspaper commentaries have run in the Chicago Tribune, the L.A. Times, the Miami Herald, and a host of other newspapers. Rothschild is the host of "[Progressive Radio](http://www.progressive.org/progressive_radio)," a syndicated half-hour weekly interview program. And he does a two-minute daily radio commentary, entitled "[Progressive Point of View](http://www.progressive.org/progressive_pov)," which is also syndicated around the country. Rothschild is the author of You Have No Rights: Stories of America in an Age of Repression (New Press, 2007). He also is the editor of Democracy in Print: The Best of The Progressive, 1909-2009(University of Wisconsin Press, 2009)., The Dangers of Obama’s Cyber War Power Grab, <http://progressive.org/dangers-of-obama-cyber-war-power-grab>

**There are no checks or balances when the President, alone, decides** when **to engage in** an act of **war**. And this new aggressive stance will lead to a cyber arms race. The **U**nited **S**tates has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves. Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the **U**nited **S**tates may use a cyberattack as the opening move in a nuclear attack. For if the **U**nited **S**tates can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight. Now, I don’t think Obama would use cyberwarfare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, **worry about the temptations of a President**.

**Fortunately, the plan solves, 2 reasons:**

**First, norm-setting — all eyes are on the U.S. —other countries model our use of OCOs — clear restrictions on use are essential — a treaty will fail**

**Bradbury 11, Assistant Attorney General for the Office of Legal Counsel**

(Steven, The Developing Legal Framework for Defensive and Offensive Cyber Operations, <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf>)

Evolving customary law. This approach also accommodates the reality that **how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.** As the label implies, **customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting** the use of its military **to the new challenges raised by computer warfare will** (and should) **help clarify the accepted customs of war in areas where the limits are not clearly established today.** And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects. For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter. Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It’s clearly not prohibited by the laws and customs of war. On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law. If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply. But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency. This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.12 There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.” And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree. At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway. Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality. The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes. Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality. Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities. The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command. Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war. The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14 **In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons.** I believe **there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations**. And **the policy decisions made by the United States** in response to particular events **will have great influence in shaping those international norms**. I think that’s the way we should want it to work.

**A notification requirement is necessary for legal norms**

**Lorber 13,** JD candidate at UPenn and PhD candidate at Duke

(Eric, EXECUTIVE WARMAKING AUTHORITY AND OFFENSIVE CYBER OPERATIONS: CAN EXISTING LEGISLATION SUCCESSFULLY CONSTRAIN PRESIDENTIAL POWER?, www.law.upenn.edu/live/files/1773-lorber15upajconstl9612013)

Should these statutes be adjusted (or new ones created) that give Congress additional oversight in this area? Two competing desiderata suggest that **oversight should be increased, but only to a limited extent**. On the one hand, policymakers have suggested that **developing strict rules and limitations on the use of offensive cyber operations will handicap the military’s ability to quickly and effectively employ these tools in critical situations, such as cyber warfare against adversarial states**. According to these arguments, developing red lines that proscribe the use of these capabilities will create reluctance and trepidation among strategists and will lead to disadvantages in combat situations. **On the other hand, developing some legal rules is necessary to ensure that, as these cyber capabilities continue to develop, the President does not gain sufficient leverage to substantially tilt the balance between the President and Congress. Moreover, because these capabilities are still developing at a fast rate, understanding how they should and should not be employed is an important goal and having senior members of Congress and their staffs— professional staff members on the intelligence committees, who** likely **have substantial experience in these areas**—**provide input would be useful in developing this understanding. These competing arguments—one for limiting any oversight and one for increasing it—suggest a middle ground that will avoid drawing red lines but will still provide useful congressional insight into the doctrinal and legal development of offensive cyber operations. Such an approach would include new legislation**, similar to the Intelligence Authorization Act, **explicitly requiring the President to report its use of covert cyber activities to the heads of Senate and House intelligence committees** (i.e. the Gang of Eight). **Congress** would not have the ability to veto such actions, however it **would be able to raise potential legal issues with the executive branch, as well as provide policy advice as to the wisdom of employing these capabilities in such circumstances**. As a result, while **the heads of these committees** would not have the ability to draw red lines themselves, they **would be able to consult with the executive branch**—as the branch employs these capabilities—**to determine their likely legality and wisdom. While the President could ignore this advice, such an approach would** at the very least **keep Congress informed of the developing capabilities and their employment. With such an approach, Congress could play a meaningful role in the shifting and uncertain legal and policy realms of offensive cyber operations, which will undoubtedly become increasingly important as the United States and other nations develop and employ these capabilities with ever-greater frequency**.

**Norms are essential to solve — they can’t be created unless OCOs are addressed**

**Goldsmith 10, Harvard Professor**, Can we stop the Cyber Arms Race, Jack Goldsmith teaches at Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. He was a member of a 2009 National Academies committee that issued the report "[Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities](http://www.anagram.com/berson/nrcoiw.pdf).", <http://articles.washingtonpost.com/2010-02-01/opinions/36895669_1_botnets-cyber-attacks-computer-attacks>

In a [speech this month on "Internet freedom](http://www.state.gov/secretary/rm/2010/01/135519.htm)," Secretary of State Hillary Clinton [decried the cyberattacks](http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html) that threaten U.S. economic and national security interests. "Countries or individuals that engage in cyber attacks should face consequences and international condemnation," she warned, alluding to the China-Google kerfuffle. We should "create norms of behavior among states and encourage respect for the global networked commons."

Perhaps so. But the problem with Clinton's call for accountability and norms on the global network -- a call frequently heard in policy discussions about cybersecurity -- is the enormous array of cyberattacks originating from the United States. Until we acknowledge these attacks and signal how we might control them, we **cannot make progress on preventing cyberattacks emanating from other countries.**

An important weapon in the cyberattack arsenal is a botnet, a cluster of thousands and sometimes millions of compromised computers under the ultimate remote control of a "master." Botnets were behind last summer's attack on South Korean and American government Web sites, as well as prominent attacks a few years ago on Estonian and Georgian sites. They are also engines of spam that can deliver destructive malware that enables economic espionage or theft.

The United States has the most, or nearly the most, infected botnet computers and is thus the country from which a good chunk of botnet attacks stem. The government could crack down on botnets, but doing so would raise the cost of software or Internet access and would be controversial. So it has not acted, and the number of dangerous botnet attacks from America grows.

The United States is also a leading source of "hacktivists" who use digital tools to fight oppressive regimes. Scores of individuals and groups in the United States design or employ computer payloads to attack government Web sites, computer systems and censoring tools in Iran and China. These efforts are often supported by U.S. foundations and universities, and by the federal government. Clinton boasted about this support seven paragraphs after complaining about cyberattacks.

Finally, the U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability. This capability remains highly classified. But the [New York Times has reported](http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2) that the Bush administration used cyberattacks on insurgent cellphones and computers in Iraq, and that it approved a plan for attacks on computers related to Iran's nuclear weapons program. And the government is surely doing much more. "We have U.S. warriors in cyberspace that are deployed overseas" and "live in adversary networks," says Bob Gourley, the former chief technology officer for the Defense Intelligence Agency.

These warriors are now under the command of Lt. Gen. Keith Alexander, director of the National Security Agency. The NSA, the world's most powerful signals intelligence organization, is also in the business of breaking into and extracting data from offshore enemy computer systems and of engaging in computer attacks that, in the NSA's words, "disrupt, deny, degrade, or destroy the information" found in these systems. When the Obama administration created "cyber command" last year to coordinate U.S. offensive cyber capabilities, it nominated Alexander to be in charge.

Simply put, the United States is in a big way doing the very things that Clinton criticized. We are not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But we are aggressively using the same or similar computer techniques for ends we deem worthy.

Our potent offensive cyber operations matter for reasons beyond the hypocrisy inherent in undifferentiated condemnation of cyberattacks. Even if we could stop all cyberattacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense. "My own view is that the only way to counteract both criminal and espionage activity online is to be proactive," [Alexander said last year](http://news.bbc.co.uk/2/hi/8033440.stm), adding that if the Chinese were inside critical U.S. computer systems, he would "want to go and take down the source of those attacks."

Our adversaries are aware of our prodigious and growing offensive cyber capacities and exploits. In a [survey published Thursday by the security firm McAfee](http://newsroom.mcafee.com/article_display.cfm?article_id=3617), more information technology experts from critical infrastructure firms around the world expressed concern about the United States as a source of computer network attacks than about any other country. This awareness, along with our vulnerability to cyberattacks, fuels a dangerous public and private cyber arms race in an arena where the offense already has a natural advantage.

**It’s reverse causal — lack of norms guarantee escalatory conflict — the U.S. is key**

**Lewis 11, Senior Fellow at CSIS** (James Andrew, Confidence-building and international agreement in cybersecurity, citizenlab.org/cybernorms2012/Lewis2011.pdf)

**Alternatives to a formal cyber treaty** began to appear as early as 2008. Rejecting formal treaties, these alternatives **drew upon the experience of global efforts to control proliferation to develop a generalized model applicable to cybersecurity. Instead of a binding legal commitment, they proposed that states develop norms for responsible state behaviour in cyberspace. Non-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behaviour. Norms shape behaviour and limit the scope of conflict. Norms create expectations and understandings among states on international behaviour, a framework for relations that provides a degree of predictability in interactions** in security, trade or politics. In this context, cybersecurity becomes the ability of states to protect their national sovereignty and advance their national interests. Cybersecurity creates new challenges for international security, as states are bound more closely together and as the perception of “transnational” risk increases, but it is largely a still undefined element in this web of relationships among states. **The idea of a norms-based approach has growing international support and, as in the nonproliferation arena, widespread adoption of norms could pave the way for more formal agreements in the future**. In July 2010 a Group of Governmental Experts (GGE) convened by the United Nations Secretary-General was able to produce an agreed report on “Developments in the Field of Information and Telecommunications in the Context of International Security”. This was unprecedented; in addition to the inability of a treaty to win consensus, a previous GGE endeavour in 2004 had failed. But the 2010 report itself is only 1,200 words long. In contrast, the first GGE had reportedly produced lengthy and detailed drafts that failed to win consensus. The brevity of the 2010 report was one element of its success (and this is a useful guidepost for future GGEs on cybersecurity), but brevity is also an indicator of the larger problems that hamper building international consensus. The successful GGE conclusion in 2010 reflected a shared perception among the government experts that **the risk of cyberconflict had become a serious threat to international peace and stability and** that **the absence of international agreement increased the risk of a destabilizing cyber incident that could spiral into a larger and more damaging conflict**. The states represented on the GGE were united by a deep concern over the possibility of **unconstrained cyberwarfare** and how this **might escalate out of control into physical violence**. They agreed that discussions of **norms** and rules **for the use of force in cyberspace**, along with other CBMs, **would improve international security and the stability of both cyberspace and the international system.** Winning even limited GGE agreement was difficult. It should be noted however that public accounts from both academic and media sources have largely glossed over significant differences expressed within the 2010 GGE. While the experts agreed on the increasing cyber threat, there was, however, little else where there was common understanding. Some states believe that **existing international norms and laws are inadequate for cyberconflict**. Other states argue that the existing laws of armed conflict are sufficient for cybersecurity, and are deeply apprehensive of doing anything that would appear to constrain freedom of speech. A central issue, as is often the case in multilateral discussion, is the extent to which states might concede a degree of sovereignty in exchange for greater security.

**Congress is key — creates transparency and legal stability — executive control snowballs**

**Harman 13, Director of the Wilson Center**

(Jane, The Extrajudicial Use of Drones: The Need for a Post-9/11 Legal Framework, www.wilsoncenter.org/article/the-extrajudicial-use-drones-the-need-for-post-911-legal-framework)

As threats, technologies, and tactics have evolved, the law has not kept up. **Before he left the White House for the CIA, John Brennan** reportedly **compiled a** highly classified “**playbook”—a set of standards to govern our counterterrorism actions.** **That’s a** necessary **short-term fix**. But, **in the long-term, Congress needs to own the game**…**and insist on transparency and legislative limits. Using new tools—particularly lethal ones—without public debate or clear legal authority is a mistake…and a slippery slope.** We need a comprehensive counterterrorism strategy across the U.S. government. Disparate tactics, with varied consequences, will not win us any friends (we’ve lost quite a few along the way)—and will not ultimately help reduce threats against the United States. In fact, **if we continue to operate without a comprehensive legal framework** around our actions, **we may end up creating more enemies than we’re eliminating.** “Why Are They the Enemy?” Consider what Gen. Stanley McChrystal, former commander of the International Security Assistance Force in Afghanistan (ISAF) and the Joint Special Operations Command, recently said about what he learned in Iraq and Afghanistan. In Iraq, he says, the first question he asked was, “Where is the enemy?'” As things evolved, the question became, “Who is the enemy?” Then “What’s the enemy doing or trying to do?'” and, finally, “Why are they the enemy?” This catechism is so revealing, but shouldn’t be surprising: the tactic of taking out bad guys may ultimately create more of them. I was recently on a panel at a security conference in Herzliya, Israel, where a thoughtful academic named Boaz Ganor discussed this so-called “boomerang effect.” The idea is that there is often a contradiction between dismantling the capability of terrorists and removing their motivation. Without a strategy and clear legal framework around our counterterrorism tactics, they can become inadvertent recruitment tools (think Gitmo). Moreover, playing whack-a-mole will not win the argument with the kid in rural Yemen deciding whether or not to strap on a suicide vest. Now that the American public is finally tuning in to the debate and insisting on clear limits on the tactics we use, Congress—the nation’s lawmakers—need to step back in. Change in Terror Threat Today, we face a horizontally organized threat. A confluence of multiple events – from reduction in al Qaeda Senior Leadership, to the rise of al Qaeda affiliates, to the new networks between Al Qaeda and among a range of extremist groups to the US drawdowns in Iraq and Afghanistan to the civil war in Syria – has changed the threat landscape tremendously. This constantly changing state of affairs – where the new “safehaven” is in many places, even hidden behind computer screens – means that the US will probably face an increase in smaller-scale attacks. To the casual observer, it may seem as though there’s been an explosion in growth of extremist terror organizations and networks in North and West Africa – Mali, Algeria, Nigeria and Morocco to name a few – but many of these groups have been around for a while. Older groups, including al Qaeda in the Islamic Maghreb, are mixing with new and taking advantage of power vacuums in many countries with weak governments. Libya hasn’t helped the situation. But these groups for the most part are opportunistic and won’t launch attacks directly on the homeland. On US citizens and installations abroad, yes, but not the U.S. homeland. But the other AQ affiliates – especially AQAP, or al Qaeda in the Arabian Peninsula – seek specifically to target the West. AQAP is also technically capable – unlike most of the other extremist groups – of plotting and carrying out complex attacks. This group also continues to publish Inspire magazine – releasing its tenth edition last month, even after the death of spiritual and operational leader Anwar al-Awlaki. Inspire dedicates many pages to proclaiming the advantages of smaller-scale attacks and provides specific instructions for carrying them out - signaling that this is the new normal. In Syria, Jabhat al Nusra has emerged as a radical faction of the Opposition. Nusra is attracting so-called “foreign fighters” easily, gaining experience and organizational skills, and without careful scrutiny, could develop into a major threat down the road. Hezbollah is often tossed by the wayside in assessments of terror threat, but historically, this group has been more lethal than al Qaeda or its affiliates. More an army than a terror group, they are better trained, better equipped, and better funded. Hezbollah is responsible for the recent attack in Bulgaria. Hezbollah attacked the US in Beirut in the 80s and the Jewish Community Center in Buenos Aires in the 90s. And Hezbollah has deep ties with the Iranian Revolutionary Guard Qods Force. Groups like Hezbollah – and even AQAP – have capabilities to carry out crude cyber attacks (think nuclear pressure controls and railroad traffic lights) as well as kinetic attacks. We can’t just worry about state actors like China, Iran and North Korea. The ranks of some terror groups are full of what I call “digital natives” – the younger generation who are tech savvy – who could easily arrange a black-market purchase of so-called “Exploits” that provide key vulnerabilities in software. To give you an example of the possible magnitude of Exploits: the “Stuxnet” virus used four of them. And they range in price, starting at an affordable $25,000 – less than half a year’s tuition! The evolution in threat means we can – and should – increasingly rely on a combination of law enforcement, counterterrorism cooperation with other countries, and limited use of kinetic power to mitigate terror threats. Tactics & Legal Authorities So, what does this evolution mean for US counterterrorism policy? First, let’s discuss the rise of “remote-control warfare”—and the failure of laws to keep up. I’m sure you’ve all seen the latest Gallup Poll data on American opinions about drones: 65% of Americans largely support drone strike against foreign terrorist suspects abroad. Only 41% support targeting Americans overseas. 25% of Americans support the prospect of domestic drone strikes. (Yikes!) But America doesn’t own the drone – or any other kind of Unmanned Aerial Vehicle. Other countries are already in the game, more than 70, in fact. The total absence of international rules for drone use is troubling, and the U.S. must take the lead and develop a strict legal framework for drone use internationally and domestically. Why are there safeguards to track communications of Americans abroad but not for killing them? **The United States has experience in constructing protective, rule-based foundations for our most sensitive programs. The framework established in the 35-year-old FISA legislation should be used** to cover targeted killings of U.S. citizens abroad and **for offensive cyber operations**. Probable cause judicial determinations used in the current FISA legal architecture can be easily applied in the context of new counterterrorism tools. Let me be clear: the “drone court” would not review operational decisions. I’m suggesting a FISA-like framework and a renamed CT court to review the criteria for making decisions to strike. As commander-in-chief, the President would determine whether and when to strike. And to answer concerns by some that the FISA court is just a rubber stamp: you may be missing the point. FISA adds judicial review to our efforts to intercept communications, which means that the Intelligence Community must go through a careful analysis and reporting process that some say can at times be “agony” and requires diligence. Yes, most cases are approved. But that ignores the large number that are not pursued because the case isn’t strong enough to meet FISA scrutiny… Inside the U.S., without exception, an American suspected of plotting a terror attack should never be targeted by an armed drone. In ''ticking-bomb’' situations – when a person in the U.S. is poised to push the button and create large-scale mayhem – SWAT teams and helicopters can do the work. This is consistent with long-standing law enforcement protocol. Second, let’s discuss new domestic surveillance capabilities: unarmed drones and cell-site simulators like the StingRay. Three years ago, when I was chair of the congressional Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, few were paying attention to moves being made by the Department of Homeland Security and a handful of U.S. police departments to use satellite imagery for routine law enforcement or emergency operations. Fortunately, Congress was able to force DHS to close its National Applications Office program that gave law enforcement access to sensitive satellites. But since that success, there has been radio silence. Except at the Federal Aviation Administration, which has been tasked with reviewing safety of domestic drones - nothing related to legal or security issues. And the federal government is forging ahead with plans to put drones into domestic airspace. DHS has a Robotic Aircraft for Public Safety Program, and it is testing multiple types of Unmanned Aerial Vehicles (UAV). After testing, DHS will transfer whatever UAV system it determines has the best capabilities for its "customers" – U.S. law enforcement. Hold on! Will law enforcement be able to fly a drone over Los Angeles or Topeka at will? How will the information gathered be used? What if increasingly capable drones can "see" into private homes and "hear" private conversations? Can such information gathered without an individualized warrant be used in a court of law? House members like Zoe Lofgren and Ted Poe have offered proposals to put in place due process protections for Americans against government-operated drones in U.S. airspace and prevent them from being armed, but their bill is far from passage. In the absence of congressional action, more than 30 state legislatures are banning or contemplating bills governing domestic drone use. But we need a national solution – not a fragmentation of state and local laws. Beyond the lack of rules for domestic drones, these vehicles are inexpensive. What’s more, the FAA predicts there may be 30,000 of them in the domestic airspace over the next decade and it may be difficult to track them – at least currently – like the drone sighting by an airline pilot in New York. Don’t get me wrong. Drone technology is not going away and it can be a very useful tool. Fire crews use drones to get a closer look at wildfires when helicopters can’t. And helicopters are expensive for police departments to maintain and fuel. But helicopters give a clear signal of their presence. Drones – in most cases – are nearly silent and can dwell longer over a particular area. Another silent tool, the “StingRay” – made famous last week in Ellen Nakashima’s Washington Post story – is a technology the American public learned about via Freedom of Information Act request. It apparently simulates a cell tower and allows collection of cell phone serial numbers and the locations of those phones. The Justice Department has said that a warrant based on probable cause is not needed to use “cell-site simulators” – like StingRay – because the government is not employing them to intercept communications. So it’s OK just to track individuals? How many other tools like this are out on the street? And what are the rules governing their use? Third, let’s discuss offensive cyber. Just two weeks ago, General Keith Alexander announced that the Department of Defense Cyber Command has created 13 offensive cyber war teams to attack computer systems and networks. No reaction. Imagine if the Pentagon announced 13 new battalions were preparing to deploy anywhere, at any time. This is a huge deal. But **there are some critical questions to raise: How will we decide whether to conduct denial of service attacks against adversaries or write malicious computer code? Does the victim of the attack matter? Will our response be different if an attack occurs on our banking system rather than our power grid? When will these teams engage? What are the red lines?** There are just too many unanswered questions. I’m thrilled that the House is planning a cyber week April 15th to consider legislation, but we also need an explanation of the current US approach to offensive cyber by the Administration. **Congress: Own the Game!** In response to abuses of the Nixon years, Congress established legislative oversight of intelligence through enacting FISA and creating the House and Senate Intel Committees. But then after 9/11, the Bush White House “leaned in” and asserted Executive power—which cut out Congress. **I’ve heard all the arguments that the President is more uniquely positioned from an institutional perspective** to exercise dexterity as it relates to national security. **However, Congress is constitutionally and structurally capable of taking the lead on laying down the ground rules.** So, what should our strategy look like? For starters, **we must review the operational framework** for new declarations of armed conflict or attacks if a group poses a sustained and organized threat to the US or its citizens. **Congress must take the lead.**

**Second it solves re-assurance — absent Congressional action it’ll be perceived as pushing the envelope**

**Dycus, Professor of National Security Law, 10**, Stephen is a Professor of national security law at Vermont Law School, former member of the National Academies committee on cyber warfare, LLM, Harvard University, LLB, BA, Southern Methodist University, “Congress’ Role in Cyber Warfare,” Journal of National Security Law & Policy, 4(1), 2010, p.161-164, <http://www.jnslp.com/read/vol4no1/11_Dycus.pdf>

In his celebrated concurring opinion in The Steel Seizure Case, **Justice Jackson cautioned that “only Congress itself can prevent power from slipping through its fingers.” Jackson’s warning seems especially pertinent today, as we prepare urgently for cyber warfare** – facing potentially enormous threats from yet unknown enemies, and finding ourselves dependent on staggeringly complex, unproven technology.3 **The executive branch**, which has special expertise and agility in national security matters generally, as well as substantial constitutional authority, **has taken the initiative in these preparations. Yet if Congress is to be faithful to the Framers’ vision of its role in the nation’s defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield**. It also must enact rules to help ensure that these policies are carried out. Congress must work hand in hand with the Executive, however, to confront these evolving threats. The importance of collaborative planning can be seen in a recent exchange of correspondence in which leaders of the Senate Select Committee on Intelligence wrote to the Director of National Intelligence to ask about “the adequacy of the Director of National Intelligence and Intelligence Community authorities over cybersecurity.” The Director answered: This is a very important issue . . . . A judgment regarding the adequacy of DNI authorities and any changes, additions, or clarifications will necessarily depend on the Administration’s strategic plan on cyber, and where the center of gravity will be within the Executive branch. . . . We have more work to do in the Executive Branch before I can give you a good answer.7 The strategic, technological, and political problems described here present challenges of unprecedented complexity. The risks of error both in the formulation of a cyber warfare policy and in its execution are substantial. And despite the importance of developing a coherent, coordinated response to this threat, it seems unlikely that we will find a way to overcome entirely the endless turf battles among federal agencies and congressional committees.8 Still, the need is so pressing and the stakes are so high that we cannot afford not to try. **The very future** of the Republic **may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves.** This article examines some of the relevant legal issues and suggests some possible solutions. I. CONGRESS’S ROLE IN DECIDING WHEN AND HOW TO GO TO WAR There is broad agreement that congressional authorization is needed to start a war. On the other hand, the President may act without Congress’s approval to repel an attack on the United States.10 Between these two extremes, the scope of the President’s unilateral authority to use military force is less well understood.11 Once hostilities are under way, there is a consensus that the President has the tactical powers of a Commander in Chief, although it may not always be clear which of the President’s actions are tactical and which are strategic.12 Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons.13 Moreover, Congress may regulate the President’s actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court’s 1800 decision in Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices in declaring that “[a]s far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations.”14 Four years later, in Little v. Barreme, the Court reiterated that the President must not exceed limits set forth in Congress’s authorization of hostilities.15 Since then, no court has ruled otherwise.16 In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR),17 which requires the President to report to Congress within 48 hours the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly approve of their continued deployment.18 Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration,19 and Congress has repeatedly referred to the WPR approvingly in subsequent legislation.20 If Congress now fails to enact guidelines for cyber warfare, it might be **perceived as inviting “measures on independent presidential responsibility**.”21 Chief Justice Marshall suggested in Little v. Barreme that if Congress had remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit.22 But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful contemporaneous role, Congress ought to **get out in front of events** now in order to be able to participate in the formulation of national policy.

**Perception of Congress is key**

**Bastby 12, Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee** (Judy, CEO of Global Cyber Risk, “U.S. Administration's Reckless Cyber Policy Puts Nation at Risk” June 4, 2012, <http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/2/>)

Perhaps **more important** **than** being out of the cyber **coordination** loop**, is the how the U.S.’s attitude is being perceived** by others **in the international community**. If the U.S. were a member of IMPACT and taking an active role in the investigation, it would be upholding its role as a global cybersecurity power. Instead, **the U.S. appears as the shirking nation** state quietly **standing on the sidelines** while being accused of engaging in cyberwarfare tactics. “**People look to the U.S., Russia, and China** **for leadership and when the U.S. is absent, they will turn to the other two**,” observes Dr. Amin. **The** U.S. **Administration’s** **failure** to **develop a strong foreign policy** **with respect to cybersecurity** **reveals** **a** gross **lack of attention at the highest levels of** the U.S. **Government** to one of the country’s most vulnerable areas — the IT systems that underpin the functioning of our society and economy. This **failure begins at basic strategy levels** **and** **extends to** reckless **disregard for the consequences** of the risky covert Stuxnet operation and failure to secure classified information about the program. For example, in May 2011, government delegations from around the world gathered in Geneva for the World Summit on the Information Society (WSIS), one of the most important communications and technology conferences globally. Noticeably, the U.S. did not have a delegation present. Yet, it was during the WSIS event that the U.S. Administration chose to release its International Strategy for Cyberspace – from Washington, D.C. rather than Geneva. WSIS participants were dumbstruck. For the few private sector Americans who were present, including myself, it was embarrassing. If in fact the Administration did authorize targeting Iranian nuclear systems with Stuxnet and/or Flame, it was a dangerous and reckless decision, especially since the U.S. Government has no idea how many computers in America may be infected with malware capable of being activated by Iran or one of its allies in retaliation. Such “backdoor” malware is capable of having enormous consequences to life and property. A similar CIA covert operation successfully destroyed a Soviet pipeline. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. The plot was revealed in a 2004 Washington Post article by David Hoffman in advance of its discussion in former Air Force Secretary Thomas C. Reed’s book, At the Abyss: An Insider’s History of the Cold War. Reed recalled to Hoffman that, “The result was the most monumental non-nuclear explosion and fire ever seen from space.” Unlike Stuxnet, however, the program remained classified for 22 years until the CIA authorized Reed to discuss it in his book. Sanger’s information came from loose-lipped persons involved with the Stuxnet operation. Before pulling a trigger (or launching malware) a nation should assess its strengths and resources and its correlation of vulnerabilities, which, in 2012, includes understanding what an adversary can do when firing back using cyber capabilities. In addition, before launching covert operations, such as Stuxnet, a nation also should ensure that the secrecy of the intelligence operations can be maintained. Conversations with Hill staffers indicate that Con**gress believes the State Department’s 2011 appointment of Coordinator for Cyber Issues has sufficiently addressed concerns** about the lack of U.S. involvement in international cybersecurity matters. Clearly, **this is narrow**, wishful **thinking**. **Congress** **needs to** stop focusing on what it believes it should force businesses to do about cybersecurity and instead focus on what it should **demand that the U.S. Government do to protect our critical infrastructure businesses and avoid retaliatory cyber attacks**. The kind of **reckless cyber diplomacy and foreign policy now at work has put our nation at risk and demonstrates cyber irresponsiblity, not cyber leadership.**

**1AC — China**

**Contention two is China:**

**Unfettered presidential control guarantees disaster for allied credibility— restoring legitimacy to OCOs is key to cyber coalitions**

**Dunlap 12**, **Major General and Former Deputy Judge Advocate General**

(Lawless Cyberwar? Not If You Want to Win, [www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html](http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html))

Military commanders have seen the no-legal-limits movie before and they do not like it. In the aftermath of 9/11, civilian lawyers moved in exactly that direction. Former Attorney General Alberto Gonzales, for example, rejected parts of the Geneva Conventions as “quaint.” He then aligned himself with other civilian government lawyers who seemed to believe that the President’s war-making power knew virtually no limits. The most egregious example of this mindset was their endorsement of interrogation techniques now widely labeled as torture.25 The results of the no-legal-limits approach were disastrous. The ill-conceived civilian-sourced interrogation, detention, and military tribunal policies, implemented over the persistent objections of America’s military lawyers, caused an international uproar that profoundly injured critical relations with indispensable allies.26 Even more damaging, they put the armed forces on the road to Abu Ghraib, a catastrophic explosion of criminality that produced what military leaders like then U.S. commander in Iraq Lieutenant General Ricardo Sanchez labeled as a “clear defeat.”27 Infused with illegalities, Abu Ghraib became the greatest reversal America has suffered since 9/11. In fact, in purely military terms, it continues to hobble counterterrorism efforts. General David Petraeus observed that “Abu Ghraib and other situations like that are non-biodegradable. They don’t go away.” “The enemy,” Petraeus says, “continues to beat you with them like a stick.”28 In short, military commanders want to adhere to the law because they have hard experience with the consequences of failing to do so. Why, then, is Baker—and others—so troubled? Actually, there are legitimate concerns about America’s cyber capabilities, but the attack on the issues is misdirected. Indeed, if Baker substitutes the term policy maker for lawyer and the term policy for law, he might be closer to the truth in terms of today’s cyberwar challenges. To those with intimate knowledge of the intricacies of cyber war, it is not the “law,” per se, that represents the most daunting issue; to them, it ispolicy. For example, retired Air Force General Michael Hayden, the former head of the National Security Agency (NSA), and later Director of the CIA, told Congress in October of 2011 that America’s cyber defenses were being undermined because cyber information was “horribly overclassified.”29 That issue is not sourced in lawyers, but in policy makers who could solve the classification problem virtually overnight if they wanted to. That same month, General Keith B. Alexander, Commander of U.S. Cyber Command and current NSA Director, said that rules of engagement were being developed that would “help to define conditions in which the military can go on the offensive against cyber threats and what specific actions it can take.” General Alexander readily acknowledges the applicability of the law of armed conflict, but suggests that challenges exist in discerning the facts and circumstances to apply to the law.30 This gets to the “act of war” question Baker complains about. The law does provide a framework;31 it is up to decision makers to discern the facts to apply to that framework. Hard to do? Absolutely. But—frankly—such “fog of war” issues are not much different than those military commanders routinely confront in the other domains of conflict where difficult decisions frequently must be made on imperfect information. The ability (or inability) to determine facts is not a legal issue, but as much a technical problem for the specialists to solve. So if there is a difficulty in that regard, the complaint ought to be directed at cyber scientists or even policy strategists, but not the lawyers. Sure, the law requires an ability to determine the source of an attack before launching a military response, but so does good sense and effective military strategy. The same can be said for the legal requirement to assess the impact on civilians and civilian objects before launching a cyber attack. This is information that decision makers would want for political and policy reasons wholly independent of any legal requirements. As the great strategist Carl von Clausewitz observed, “War is the continuation of policy by other means.”32 Again, if the ability to make the calculations that political leaders and policy makers require as much as lawyers is inadequate, that is a technical, not legal, issue. When—and if—the facts and circumstances are determined, weighing them is what policy makers and military commanders “do.” Lawyers may help them, but ultimately it is the decision maker’s call, not the lawyer’s. Any reluctance of decision makers to make difficult fact determinations—if such reluctance does exist—is not, in any event, a deficiency of law, but ofleadership. Of course, such decisions are never exclusively about legal matters. Policy makers and commanders rightly take into account a variety of factors beyond the law. In actual practice, it appears that such considerations often are more limiting than the law. For example, the Washington Post reported that U.S. cyber weapons “had been considered to disrupt Gaddafi’s air defenses” early in NATO’s UN-sanctioned operations aimed at protecting Libyan civilians.33 However, the effort “was aborted,” the Post said, “when it became clear that there was not enough time for a cyber attack to work.” Conventional weapons, it was said, were “faster, and more potent,” a pure military rationale. None of this reflects even the slightest suggestion that “lawyers” or the law frustrated the execution of a cyber operation in Libya. No doubt there was discussion about cyber-reporting obligations under the War Powers Resolution, but Presidents have almost never seen that as a bar to military actions, so it can hardly be said to be something unique to cyber operations or that operated to actually block a cyber attack, per se. Rather, it is but one of the many political considerations applicable to military actions generally, cyber or otherwise. To be clear, the primary concern about the potential use of cyber weaponry against Libya wasnot anything generated by lawyers as Baker might put it, but rather by “administration officials and even some military officers” who, the New York Times says, “balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own.” Along this line, the Times quoted James Andrew Lewis, a senior fellow at the Center for Strategic and International Studies, as opining that the United States does not want to be the “ones who break the glass on this new kind of warfare.”34 Again, the legitimacy of these concerns aside, they illustrate— regardless—that while there may be unresolved policy questions inhibiting cyber operations, that is altogether different from the legal problems of Baker’s imaginings. The threat of cyberwar is certainly an extremely serious one, but surely not a greater peril than is nuclear war. Yet at least insofar as the U.S. military is concerned, nuclear operations can be made amenable to the law.35 In other words, if our survival does not require abandoning the rule of law with respect to nuclear weapons, there is certainly no reason to do so in the cyber realm. Does Baker nevertheless believe that the United States is so vulnerable to catastrophic cyber attack that the nation must reject any legal limits in its cyber response? If, indeed, the United States were as vulnerable to catastrophic attack as Baker would have us believe, al Qaeda or some extremist group certainly would have launched one by now. In point of fact, although cyber crime may be extensive, militarily significant cyber attacks apparently are not so easy to conduct as Baker seems to think. In reporting the rejection of cyber weaponry as a means of dismantling ibyan air defenses, The New York Times noted that: **While** popular fiction and **films depict cyberattacks as easy to mount**—only a few computer keystrokes needed—**in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes**. Obviously, **if cyber weaponry is technically difficult for the world’s foremost military to use even against a third-world power such as Libya, one may reasonably infer that it is markedly more difficult to use against a sophisticated first-world power**, even for a peer or near peer of that power. **Rejection of legal limits carries** other, **real-world consequences that are not in the United States’ cyber interests. An effective response to cyber threats is not an autarchic enterprise; it requires the cooperation of international allies**. Baker’s “**damn the law** and lawyers” **approach would cripple our relations with the law-abiding nations whose cooperation we must have to address cyber threats.** We need to keep in mind that the vast majority of adverse cyber incidents are criminal matters, and the resolution of them frequently necessitates the involvement of foreign police and judicial authorities who, by definition, require partners who are themselves committed to faithfulness to the rule of law. **The importance of legal legitimacy cannot be overstated**. As outlined above, **few in uniform who have experienced the vicissitudes of war since 9/11 would underestimate the deleterious impact on coalition support that the mere perception of American lawlessness can have.**

**The small concession of the plan is key — it increases key flexibility and secures cyberspace**

**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 United States should lead a broad**, multi-stakeholder **international cyber security** **coalition** **that supplements U.S. freedom of action** in cyberspace with global norms that will help protect its interests. **The United States must play a greater leadership role** within a range of existing and emerging international coalitions **if it wishes to shape the future of cyberspace** and how it is governed.35 **Exercising leadership** may, in some circumstances, **require the United States to curtail** some **freedom of action** internationally in order to shape the behavior of others. It does this already by adhering to existing norms and agreements, such as the Law of Armed Conflict and World Trade Organization. As long as such tradeoffs remain consistent with American interests and values, **this cooperative leadership model offers** **the best way for the United States to strengthen its cyber security**. Since the United States pursues competing interests and values in cyberspace, **it must develop policies that balance those** interests **and values**. An effective cyber security strategy **requires** American **policymakers to balance competing interests** and values in a way that defends the nation without subverting what it stands for.

**Chinese anti-access capabilities critically depend on cyber — allied cooperation is key to counter them**

**Kazianis 12, Fellow at the CSIS Pacific Forum**, is Assistant Editor for The Diplomat and a non-resident fellow at the Pacific Forum: CSIS. The views expressed in this article are those of the author and do not reflect the position of The Diplomat or Pacific Forum., <http://csis.org/files/publication/Pac1241A.pdf>

US Secretary of Defense Leon Panetta warned that the “next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems.” If true, cyber must be front and center in any military refocusing to the Asia-Pacific. Any failure to not correctly plan against this lethal form of asymmetric warfare could be a catastrophic mistake. The US seems to be focusing the military component of its widely discussed ‘pivot’ to Asia on China’s growing military capabilities. While neither side seeks confrontation and one hopes none will occur, China’s development of a highly capable Anti-Access/Area Denial (A2/AD) battle plan to deter, slow, or deny entry into a contested geographic area or combat zone has been detailed extensively. Cyber war is clearly part of this strategy, with Chinese planners prepared to wage ‘local wars under conditions of informatization,’ or highintensity, information-centric regional military operations of short duration. Prudent military planners must be prepared to meet this potential threat. Other nations such as North Korea and Iran are also developing A2/AD capabilities with cyber based components that could challenge US or allied interests. In this type of threat environment, the US, along with its allies, should develop its own symmetric and asymmetric counter-strategies. A joint operational concept of AirSea Battle that includes a strong cyber component would give US forces and their allies the **best chance to defeat adversary A2/AD forces**. Of course, the current Joint Operational Access Concept does make strong mention of cyber operations. However, an even stronger emphasis on cyber warfare is needed. In short, AirSea Battle as an operational concept might already be obsolete and it should be reconstituted as an “AirSeaCyber” concept. If cyber is to become a full-fledged component of AirSea Battle, its conceptualization and integration are crucial. A simple first step must be the recognition that cyberspace is now one of the most important battlefield domains in which the US and allied militaries operate. It is not enough to exercise battlefield dominance in a physical sense with technologically advanced equipment. With vital but vulnerable computer networks, software, and operating systems a potential adversary may choose an asymmetric cyber ‘firststrike’ to damage its opponent’s networked combat capabilities. Enemy forces could attempt to ‘blind’ their opponent by crippling computer and network-centric command and control (C2), battlefield intelligence gathering, and combat capabilities by conducting advanced cyber operations. Simply put: US and allied forces must fully understand and articulate the severity of the threat they face before they can map out any national or multinational strategies. Working with potential cyber allies to identify common threats and working to mitigate possible challenges is crucial. One viable partner in creating effective cyber capabilities is South Korea. Seoul faces a number of problems from a growing North Korean asymmetric threat in a physical sense, as well as multiple challenges in cyberspace. General James Thurman, US Forces Korea Commander, recently noted that “North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber-attacks.” Pyongyang utilizes cyber capabilities “against a variety of targets including military, governmental, educational and commercial institutions.” With the US committed to South Korea’s defense, creating partnerships in cyberspace can only enhance such a relationship. Both sides must look past physical threats and expand their partnership across this new domain of possible conflict. Japan is another possible cyberspace partner. As Matsubara accurately points out, “They [US and Japan] have more to lose. If cyber-attacks and espionage undermine their economies or military capability, **larger geostrategic balances may be affected** and the negative consequences may spill over to other countries.” Both nations have reported hacking incidents from Chinese-based hackers that have targeted defense-related industries and programs. With Japan and the US partnering on joint projects such as missile defense and F- 35 fighter jet, the protection of classified information associated with these programs must be a top priority. As military allies, both must plan for possible regional conflict where cyber warfare could be utilized against them. Sadly, restraints could develop that might hamper such partnerships. One recent example: historical and political tensions have delayed and possibly halted a defense agreement between Japan and South Korea. The pact would have assisted in the direct sharing of sensitive military information concerning North Korea, China, and missile defenses. Presumably, cyber-related information would have been at the center of such sharing. The agreement was supported by Washington, which has been working to reinforce trilateral cooperation with the two countries, as essential Asian allies.

**China’s rapidly modernizing its military for an A2AD strategy — that fuels territorial disputes**

**RTT 13**, China’s Anti-access And Area-denial Capabilities Bolstered: Pentagon Report, <http://www.rttnews.com/2111200/china-s-anti-access-and-area-denial-capabilities-bolstered-pentagon-report.aspx>

A new report of the U.S. Defense Department says that China is increasing its rapid military modernization program, and that the advanced technologies bolster China's anti-access and area-denial capabilities.

The annual report -- titled "2013 Military and Security Developments Involving the People's Republic of China" -- was submitted to the Congress on Monday. It covers China's security and military strategies; developments in its military doctrine, force structure and advanced technologies; the security situation in the Taiwan strait; U.S.-China military-to-military contacts and the U.S. strategy for such engagement; and the nature of China's cyber activities directed against the Defense Department.

David F. Helvey, Deputy Assistant Secretary of Defense for East Asia, briefed Pentagon reporters on the report. He noted that the report, which DoD coordinates with other agencies, "reflects broadly the views held across the United States government." The report is factual and not speculative, he noted.

Helvey said the trends in this year's report show "a good deal of continuity in terms of the modernization priorities (of China)," despite the 2012 and 2013 turnover to new leadership in that Communist country.

The document notes that China has launched its first aircraft carrier in 2012 and has been **sustaining investments** in advanced short- and medium-range conventional ballistic missiles, land-attack and anti-ship cruise missiles, counter-space weapons and military cyberspace systems.

"The issue here is not one particular weapons system. It's the integration and overlapping nature of these weapons systems into a regime that can potentially impede or restrict free military operations in the Western Pacific. So that's something that we monitor and are concerned about," Helvey said.

The report provided a lot of information, but also raises some questions. "What concerns me is the extent to which China's military modernization occurs in the absence of the kind of openness and transparency that others are certainly asking of China," he added.

That lack of transparency has effects on the security calculations of others in the region, "and that's of greater concern," he noted.

Addressing China's cyber capabilities, Helvey said "in 2012, numerous computer systems around the world, including those owned by the United States government, continued to be targeted for intrusions, some of which appear to be attributable directly to [Chinese] government and military organizations."

The report noted that China has "increased assertiveness with respect to its maritime territorial claims" over the past year. **China disputes sovereignty with Japan over islands in the East China Sea, and has other territorial disputes with regional neighbors in the South China Sea**.

**PLA doctrine proves Chinese aggression against Taiwan and the South China Sea are inevitable — A2AD is the linchpin of this capability**

**Yoshihara 10** (Dr. Toshi Yoshihara, Associate Professor in the Strategy and Policy Department at the Naval War College, former Visiting Professor at the U.S. Air War College, Ph.D. International Relations, The Fletcher School of Law and Diplomacy, Tufts University, M.A. International Relations, School of Advanced International Studies, Johns Hopkins University, B.S. International Relations, School of Foreign Service, Georgetown University, “Chinese Missile Strategy and the U.S. Naval Presence in Japan: The Operational View from Beijing,” Naval War College Review, 7-1-2010, (... denotes non-US-ASCII text omitted) <http://www.faqs.org/periodicals/201007/2046727461.html>)
In recent years, defense analysts in the United States have substantially revised their estimates of China's missile prowess. A decade ago, most observers rated Beijing's ballistic missiles as inaccurate, blunt weapons limited to terrorizing civilian populations. Today, the **emerging consensus** within the U.S. strategic community is that China's arsenal can inflict lethal harm with precision on a wide range of military targets, including ports and airfields. As a consequence, many observers have jettisoned previously sanguine net assessments that conferred decisive, qualitative advantages to Taiwan in the cross-strait military balance. Indeed, the debates on China's coercive power and Taiwan's apparent inability to resist such pressure have taken on a palpably fatalistic tone. A 2009 RAND monograph warns that China's large, modern missile and air forces are likely to pose a virtually insurmountable challenge to Taiwanese and American efforts to command the air over the strait and the island. The authors of the report believe that massive ballistic-missile salvos launched against Taiwan's air bases would severely hamper Taipei's ability to generate enough fighter sorties to contest air superiority. They state: "As China's ability to deliver accurate fire across the strait grows, it is becoming increasingly difficult and soon may be impossible for the United States and Taiwan to protect the island's military and civilian infrastructures from serious damage."1 As a result, the authors observe, "China's ability to suppress Taiwan and local U.S. air bases with ballistic and cruise missiles seriously threatens the defense's ability to maintain control of the air over the strait."2 They further assert, "The United States can no longer be confident of winning the battle for the air in the air. This represents a dramatic change from the first five-plus decades of the China- Taiwan confrontation."3 An unclassified Defense Intelligence Agency report assessing the state of Taiwan's air defenses raises similar concerns. The study notes that Taiwanese fighter aircraft would be unable to take to the air in the absence of well-protected airfield runways, suggesting a major vulnerability to the island's airpower. The agency further maintains that Taiwan's capacity to endure missile attacks on runways and to repair them rapidly will determine the integrity of the island's air-defense system.4 While the report withholds judgment on whether Taipei can maintain air superiority following Chinese missile strikes in a conflict scenario, a key constituent of the U.S. intelligence community clearly recognizes a growing danger to Taiwan's defense. China's missiles also threaten Taiwan's ability to defend itself at sea. William Murray contends that China could sink or severely damage many of Taiwan's warships docked at naval piers with salvos of ballistic missiles. He argues that "the Second Artillery's [China's strategic missile command's] expanding inventory of increasingly accurate [short-range ballistic missiles] probably allows Beijing to incapacitate much of Taiwan's navy and to ground or destroy large portions of the air force in a surprise missile assault and follow-on barrages."5 These are stark, sobering conclusions. Equally troubling is growing evidence that China has turned its attention to Japan, home to some of the largest naval and air bases in the world. Beijing has long worried about Tokyo's potential role in a cross-strait conflagration. In particular, Chinese analysts chafe at the apparent American freedom to use the Japanese archipelago as a springboard to intervene in a Taiwan contingency. In the past, China kept silent on what the People's Liberation Army (PLA) would do in response to Japanese logistical support of U.S. military operations. **Recent PLA publications**, in contrast, suggest that the logic of missile coercion against Taiwan could be readily applied to U.S. forward presence in Japan. The writings convey a **high degree of confidence** that China's missile forces could compel Tokyo to limit American use of naval bases while selectively destroying key facilities on those bases. These doctrinal developments demand close attention from Washington and Tokyo, lest the transpacific alliance be caught flat-footed in a future crisis with Beijing. This article is a first step toward better understanding how the Chinese evaluate the efficacy of missile coercion against American military targets in Japan. This article focuses narrowly on Chinese assessments of U.S. naval bases in Japan, excluding the literature on such other key locations as the Kadena and Misawa air bases. The writings on the American naval presence are abundant and far more extensive than studies on the land and air components of U.S. basing arrangements. The dispatch of two carrier battle groups to Taiwan's vicinity during the 1996 cross-strait crisis stimulated Beijing's reevaluation of its military strategy toward the island. Not surprisingly, the Chinese are obsessed with the U.S. aircraft carrier, including the facilities and bases that support its operations. It is against this rich milieu that this study explores how the Chinese conceive their missile strategy to complicate American use of military bases along the Japanese archipelago. This article first explores the reasons behind Beijing's interest in regional bases and surveys the Chinese literature on the U.S. naval presence in Japan to illustrate the amount of attention being devoted to the structure of American military power in Asia. **Chinese analysts see U.S. dependence on a few locations for power projection as a major vulnerability**. Second, it turns to Chinese **doctrinal publications, which furnish astonishing details** as to how the PLA might employ ballistic missiles to complicate or deny U.S. use of Japanese port facilities. Chinese defense planners place substantial faith in the coercive value of missile tactics. Third, the article assesses China's conventional theater ballistic missiles that would be employed against U.S. regional bases. Fourth, it critiques the Chinese writings, highlighting some faulty assumptions about the anticipated effects of missile coercion. Finally, the study identifies some key operational dilemmas that the U.S.-Japanese alliance would likely encounter in a PLA missile campaign. EXPLAINING CHINA'S INTEREST IN REGIONAL BASES Taiwan remains the animating force behind China's strategic calculus with respect to regional bases in Asia. Beijing's inability to respond to the display of U.S. naval power at the height of the 1996 Taiwan Strait crisis proved highly embarrassing. There is evidence that the PLA had difficulty in monitoring the movement of the two carrier battle groups, much less in offering its civilian leaders credible military options in response to the carrier presence. This galling experience **steeled Beijing's resolve** to preclude U.S. naval deployments near Taiwan in a future crisis. Notably, the Yokosuka-based USS Independence (CV 62) was the first carrier to arrive at the scene in March 1996, cementing Chinese expectations that Washington would dispatch a carrier from Japan in a contingency over Taiwan. Beyond Taiwan, other territorial disputes along China's nautical periphery could involve U.S. naval intervention. A military crisis arising from conflicting Sino-Japanese claims over the Senkaku (Diaoyu) islands northwest of Taiwan could compel an American reaction. While doubts linger in some Japanese policy circles as to whether foreign aggression against the islands would trigger Washington's defense commitments as stipulated by the U.S.-Japanese security treaty, joint allied exercises and war games since 2006 suggest that the U.S. military is closely watching events in the East China Sea. Farther south, Chinese territorial claims over large swaths of the South China Sea could also be **sources of regional tensions. If a local tussle there escalated into a larger conflagration that threatened international shipping**, the U.S. Navy might be ordered to maintain freedom of navigation. In both scenarios, the U.S. carrier based in Japan and other strike groups operating near Asian waters would be called upon as first responders. Concrete territorial disputes that have roiled Asian stability are not the only reasons that American naval power would sortie from regional bases to the detriment of Chinese interests. More abstract and esoteric dynamics may be at work. For example, Chinese leaders fret about the so-called Malacca dilemma. China's heavy dependence on seaborne energy supplies that transit the Malacca Strait has set off Chinese speculation that the United States might seek to blockade that maritime choke point to coerce Beijing.6 This insecurity stems less from judgments about the possibility or feasibility of such a naval blockade than from the belief that a great power like China should not entrust its energy security to the fickle goodwill of the United States. If the U.S. Navy were ever called upon to fulfill an undertaking of such magnitude, forward basing in Asia would undoubtedly play a pivotal role in sustaining what could deteriorate into a protracted blockade operation. Chinese analysts have also expressed a broader dissatisfaction with America's self-appointed role as the guardian of the seas. Sea-power advocates have vigorously pushed for a more expansive view of China's prerogatives along the maritime periphery of the mainland. They bristle at the U.S. Navy's apparent presumption of the right to command any parcel of the ocean on earth, including areas that China considers its own nautical preserves. Some take issue with the 2007 U.S. maritime strategy, a policy document that baldly states, "We will be able to impose local sea control wherever necessary, ideally in concert with friends and allies, but by ourselves if we must."7 Lu Rude, a former professor at Dalian Naval Academy, cites this passage as evidence of U.S. "hegemonic thinking." He concludes, "Clearly, what is behind 'cooperation' is America's interests, having 'partners or the participation of allies' likewise serves America's global interests."8 Some Chinese, then, object to the very purpose of U.S. sea power in Asia, which relies on a constellation of regional bases for its effects to be felt (see map). Long-standing regional flash points and domestic expectations of a more assertive China as it goes to sea suggest that Beijing's grudging acceptance of U.S. forward presence could be eroding even more quickly than once thought. Against this backdrop of increasing Chinese ambivalence toward American naval power, U.S. basing arrangements in Japan have come into sharper focus. CHINESE VIEWS OF U.S. NAVAL BASES IN JAPAN Some Chinese strategists appraise Washington's military posture in the Asia-Pacific region in stark geopolitical terms. Applying the "defense perimeter of the Pacific" logic elaborated by Secretary of State Dean Acheson in the early Cold War, they see their na - tion enclosed by concentric, layered "island chains." The United States and its allies, they argue, can encircle China or blockade the Chinese mainland from island strongholds, where powerful naval expeditionary forces are based. Analysts who take such a view conceive of the island chains in various ways. Yu Yang and Qi Xiaodong, for example, describe U.S. basing architecture in Asia as a "three line configuration [...]."9 The first line stretches in a sweeping arc from Japan and South Korea to Diego Garcia in the Indian Ocean, forming a "zone of forward bases[...]." This broad notion that the U.S. presence in the western Pacific and the Indian Ocean constitutes a seamless, interlocking set of bases is widely shared in Chinese strategic circles.10 The second line connects Guam and Australia. The last line of bases runs north from Hawaii through Midway to the Aleutians, terminating at Alaska. While these island chains may bear little resemblance to actual U.S. thinking and planning, that the Chinese pay such attention to the geographic structure of American power in Asia is quite notable. These observers discern a cluster of mutually supporting bases, ports, and access points along these island chains. Among the networks of bases in the western Pacific, those located on the Japanese archipelago-the northern anchor of the first island chain-stand out, for the Chinese. Modern Navy, a monthly journal published by the Political Department of the People's Liberation Army Navy, produced a seven-part series on Japan's Maritime Self-Defense Force in 2004 and 2005. Notably, it devoted an entire article to Japan's main naval bases, including Yokosuka, Sasebo, Kure, and Maizuru.11 The depth of the coverage of these bases is rather remarkable, especially when compared to the sparse reporting on similar topics in the United States and in Japan. Perhaps no other place captures the Chinese imagination as much as Yokosuka, which analysts portray as the centerpiece of U.S. basing in Asia.12 One analysis depicts a "Northeast Asian base group [...]" radiating outward from Yokosuka to Sasebo, Pusan, and Chinhae.13 Writers provide a wide range of details about the Yokosuka naval base, including its precise location, the surrounding geography, the number of piers (particularly those suitable for aircraft carriers), the types and number of maintenance facilities, and the storage capacity of munitions, fuel, and other supply depots.14 Wu Jian, for instance, finds the geographic features of Yokosuka comparable to those of Dalian, a major base of the Chinese navy's North Sea Fleet.15 Beyond physical similarities, Yokosuka evokes unpleasant memories for the Chinese. One commentator recalls the U.S. transfer of 203 mm heavy artillery from Yokosuka to Nationalist forces on Jinmen during the 1958 Taiwan Strait crisis.16 Tracking more recent events, another observer notes that the Kitty Hawk Strike Group's deployments from Yokosuka to waters near Taiwan invariably coincided with the presidential elections on the island, in 2000, 2004, and 2008.17 As Pei Huai opines, "Yokosuka has all along irritated the nerves of the Chinese people."18 Moreover, Chinese analysts are keenly aware of Yokosuka's strategic position. As Du Chaoping asserts: Yokosuka is the U.S. Navy's main strategic point of concentration and deployment in the Far East and is the ideal American stronghold for employing maritime forces in the Western Pacific and the Indian Ocean regions. A carrier deployed there is akin to the sharpest dagger sheathed in the Western Pacific by the U.S. Navy. It can control the East Asian mainland to the west and it can enter the Indian Ocean to the southwest to secure Malacca, Hormuz, and other important thoroughfares.19 Ma Haiyang concurs: The Yokosuka base controls the three straits of Soya, Tsugaru, Tsushima and the sea and air transit routes in the Indian Ocean. As the key link in the "island chain," it can support ground operations on the Korean Peninsula and naval operations in the Western Pacific. It can support combat in the Middle East and Persian Gulf regions while monitoring and controlling the wide sea areas of the Indian Ocean. Its strategic position is extremely important.20 It is notable that both Du and Ma conceive of Yokosuka as a central hub that tightly links the Pacific and Indian oceans into an integrated theater of operations. Intriguingly, some Chinese commentators view Yokosuka as the front line of the U.S.-Japanese defense cooperation on missile defense. They worry that Aegis-equipped destroyers armed with ballistic-missile-defense (BMD) systems based in Yokosuka could erode China's nuclear deterrent. Indeed, analysts see concentrations of sea-based BMD capabilities falling roughly along the three island chains described above. Ren Dexin describes Yokosuka as the first line of defense against ballistic missiles, while Pearl Harbor and San Diego provide additional layers.21 Yokosuka is evocatively portrayed as the "forward battlefield position" (...), the indispensable vanguard for the sea-based BMD architecture.22 For some Chinese, these concentric rings or picket lines of sea power appear tailored specifically to bring down ballistic missiles fired across the Pacific from locations as diverse as the Korean Peninsula, 1mainland China, India, or even Iran.23 Specifically, Aegis ships in Yokosuka, Pearl Harbor, and San Diego would be positioned to shoot down missiles in their boost, midcourse, and terminal phases, respectively.24 Chinese observers pay special attention to Aegis deployments along the first island chain. Some believe that Aegis ships operating in the Yellow, East, and South China seas would be able to monitor the launch of any long-range ballistic missile deployed in China's interior and perhaps to intercept the vehicle in its boost phase. Dai Yanli warns, "Clearly, if Aegis systems are successfully deployed around China's periphery, then there is the possibility that China's ballistic missiles would be destroyed over their launch points."25 Ji Yanli, of the Beijing Aerospace Long March Scientific and Technical Information Institute, concurs: "If such [seabased BMD] systems begin deployment in areas such as Japan or Taiwan, the effectiveness of China's strategic power and theater ballistic-missile capabilities would weaken tremendously, severely threatening national security."26 Somewhat problematically, the authors seemingly assume that Beijing would risk its strategic forces by deploying them closer to shore, and they forecast a far more capable Aegis fleet than is technically possible in the near term. The indispensability of the ship-repair and maintenance facilities at Yokosuka emerges as another common theme in the Chinese literature. Analysts in China often note that Yokosuka is the only base west of Hawaii that possesses the wherewithal to handle major carrier repairs. Some have concluded that Yokosuka is irreplaceable as long as alternative sites for a large repair station remain unavailable. Li Daguang, a professor at China's National Defense University and a frequent commentator on naval affairs, casts doubt on Guam as a potential candidate, observing that the island lacks the basic infrastructure and economies of scale to service carriers.27 China's Jianchuan Zhishi (Naval and Merchant Ships) published a translated article from a Japanese military journal, Gunji Kenkyu (Japan Military Review), to illustrate the physical limits of Guam as a permanent home port for carriers.28 Chinese analysts also closely examine Sasebo, the second-largest naval base in Japan. Various commentators call attention to its strategic position near key sea-lanes and its proximity to China.29 As Yu Fan notes, "This base is a large-scale naval base closest to our country. Positioned at the intersection of the Yellow Sea, the East China Sea, and the Sea of Japan, it guards the southern mouth of the Korea Strait. This has very important implications for controlling the nexus of the Yellow Sea, the East China Sea, and the Sea of Japan and for blockading the Korea Strait."30 It is clear, then, that Chinese strategists recognize the importance of U.S. naval bases in Japan for fulfilling a range of regional and extraregional responsibilities. Indeed, some believe that the American strategic position in Asia hinges entirely on ready military access to bases on the Japanese islands. Tian Wu argues that without bases in Japan, U.S. forces would have to fall back to Guam or Hawaii. Tian bluntly asserts: If the U.S. military was ever forced to withdraw from Okinawa and Japan, then it would be compelled to retreat thousands of kilometers to set up defenses on the second island chain. Not only would it lose tremendous strategic defensive depth, but it would also lose the advantageous conditions for conducting littoral operations along the East Asian mainland while losing an important strategic relay station to support operations in the Indian Ocean and the Middle East through the South China Sea.31 This emerging discourse offers several clues about Beijing's calculus in regard to U.S. naval basing arrangements in Japan. Chinese strategists see these bases as collectively representing both a threat to Chinese interests and a critical vulnerability for the United States. Bases in Japan are the most likely locations from which the United States would sortie sea power in response to a contingency over Taiwan. At the same time, the Chinese are acutely aware of the apparent American dependence on a few bases to project power. Should access to and use of these bases be denied for political or military reasons, they reason, Washington's regional strategy could quickly unravel. While the commentaries documented above are by no means authoritative in the official sense, they are clearly designed to underscore the strategic value and the precariousness of U.S. forward presence in Japan. U.S. BASES IN JAPAN AND CHINESE MISSILE STRATEGY Authoritative PLA documents correlate with this emerging consensus that U.S. bases on the Japanese home islands merit close attention in strategic and operational terms. Indeed, Chinese doctrinal writings clearly indicate that the American presence in Japan would likely be the subject of attack if the United States were to intervene in a cross-strait conflict. The unprecedented public availability of primary sources in China in recent years has opened a window onto Chinese strategic thought, revealing a genuinely competitive intellectual environment that has substantially advanced Chinese debates on military affairs. This growing literature has also improved the West's understanding of the PLA. In an effort to maximize this new openness in China, this article draws upon publications closely affiliated with the PLA, including those of the prestigious Academy of Military Science and the National Defense University, that address coercive campaigns against regional bases in Asia.32 Some are widely cited among Western military analysts as authoritative works that reflect current PLA thinking. Some likely enjoy official sanction as doctrinal guidance or educational material for senior military commanders. The authors of the studies are high-ranking PLA officers who are either leading thinkers in strategic affairs and military operations or boast substantial operational and command experience. These works, then, collectively provide a sound starting point for examining how regional bases in Asia might fit into Chinese war planning. Among this literature, The Science of Military Strategy stands out in Western strategic circles as an authoritative PLA publication. The authors, Peng Guangqian and Yao Youzhi, advocate an indirect approach to fighting and prevailing against a superior adversary in "future local wars under high-technology conditions."33 To win, the PLA must seek to avoid or bypass the powerful field forces of the enemy while attacking directly the vulnerable rear echelons and command structures that support frontline units. Using the human body as an evocative metaphor for the adversary, Peng and Yao argue, "As compared with dismembering the enemy's body step by step, destroying his brain and central nerve system is more meaningful for speeding up the course of the war."34 To them, the brain and the central nervous system of a war machine are those principal directing and coordinating elements without which the fighting forces wither or collapse. The aim, then, is to conduct offensive operations against the primary sources of the enemy's military power, what the authors term the "operational system." They declare, "After launching the war, we should try our best to fight against the enemy as far away as possible, to lead the war to enemy's operational base, even to his source of war, and to actively strike all the effective strength forming the enemy's war system."35 In their view, operational systems that manage command and control and logistics (satellites, bases, etc.), are the primary targets; they relegate tactical platforms that deliver firepower (warships, fighters, etc.) to a secondary status. To illustrate the effects of striking the source of the enemy's fighting power, Peng and Yao further argue: To shake the stability of enemy's war system so as to paralyze his war capabilities has already become the core of the contest between the two sides in the modern hightech local war. So, more attention should be paid to striking crushing blows against the enemy's structure of the operational system . . . especially those vulnerable points which are not easy to be replaced or revived, so as to make the enemy's operational system seriously unbalanced and lose initiative in uncontrollable disorder.36 The authors are remarkably candid about what constitutes the enemy's operational system. Particularly relevant to this study is their assertion that the supply system emerges as a primary target: The future operational center of gravity should not be placed on the direct confrontation with the enemy's assault systems. We should persist in taking the information system and support system as the targets of first choice throughout. . . . In regard to the supply system, we should try our best to strike the enemy on the ground, cut the material flow of his efficacy sources so as to achieve the effect of taking away the firewood from the caldron.37 Destruction of the supply system in effect asphyxiates the adversary. In order to choke off the enemy's capacity to wage war, Peng and Yao contend, a "large part of the supply systems must be destroyed."38 Their prescriptions for winning local high-tech wars suggest that the horizontal escalation of a conflict to U.S. regional bases in Asia is entirely thinkable. Even more troubling, some Chinese appear to envision the application of substantial firepower to pummel the U.S. forward presence. While The Science of Military Strategy should not be treated as official strategic guidance to the PLA, its conceptions of future conflict with a technologically superior adversary provide a useful framework for thinking about what a Chinese missile campaign against regional bases might entail. There is substantial evidence in Chinese doctrinal writings that PLA defense planners anticipate the possibility of a sizable geographic expansion of the target set, to include U.S. forward presence in East Asia. Although the documents do not explicitly refer to naval bases in Japan, they depict scenarios strongly suggesting that Yokosuka is a primary target. In the hypothetical contingencies posited in these writings, U.S. intervention is a critical premise, if not a given. In particular, Chinese planners expect Washington to order the deployment of carrier strike groups near China's coast, a prospect that deeply vexes Beijing. It is in this context of a highly stressful (though by no means inconceivable) scenario that U.S. military bases come into play in Chinese operational thinking. **For PLA planners, the primary aims are to deter, disrupt, or disable the employment of carriers** at the point of origin, namely, the bases from which carriers would sortie. Given the limited capability, range, and survivability of China's air and sea power, **most studies foresee the extensive use of long-range conventional ballistic missiles to achieve key operational objectives** against U.S. forward presence. In Intimidation Warfare, Zhao Xijun proposes several novel missile tactics that could be employed to deter the use of naval bases in times of crisis or war.39 Zhao proposes demonstration shots into sea areas near the enemy state to compel the opponent to back down. Zhao explains, "Close-in (near border) intimidation strikes involve firing ballistic missiles near enemy vessels or enemy states (or in areas and sea areas of enemy-occupied islands). It is a method designed to induce the enemy to feel that it would suffer an unbearable setback if it stubbornly pursues an objective, and thus abandons certain actions."40 One tactic that Zhao calls a "pincer, close-in intimidation strike" is particularly relevant to missile options against U.S. military bases. Zhao elaborates: "Pincer close-in intimidation strikes entail the firing of ballistic missiles into the sea areas (or land areas) near at least two important targets on enemy-occupied islands (or in enemy states). This enveloping attack, striking the enemy's head and tail such that the enemy's attention is pulled in both directions, would generate tremendous psychological shock."41 Zhao also proposes an "island over-flight attack" as a variation of the pincer strike. He states: For high-intensity intimidation against an entrenched enemy on an island, an island over-flight attack employs conventional ballistic missiles with longer range and superior penetration capabilities to pass over the enemy's important cities and other strategic targets to induce the enemy to sense psychologically that a calamity will descend from the sky. This method could produce unexpected effects.42 While these missile tactics are primarily aimed at coercing Taiwan, they could also, in theory, be applied to any island nation. Reminiscent of the 1996 crossstrait crisis, the PLA could splash single or multiple ballistic missiles into waters near Yokosuka (shot across Honshu Island, over major metropolitan cities) in the hopes that an intimidated leadership in Tokyo would stay out of a contingency over Taiwan, deny American access to military facilities, or restrict U.S. use of naval bases in Japan. Should deterrence through intimidation fail, the Chinese may seek to complicate U.S. naval operations originating from bases located in the Japanese home islands. The Science of Second Artillery Campaigns, the most authoritative work on the PLA's strategic rocket forces, furnishes astonishingly vivid details on the conditions under which China might seek to conduct conventional missile operations against outside intervention.43

**Taiwan crisis is imminent and causes nuclear war — it’s the most probable**

**Colby and Denmar, et al 13**, Elbridgc A. Colby. cochair, is a principal analyst and drvison lead for global strategic affairs at the Center for Naval Analyses (CNA). where he focuses on strateg deterrence, nuclear weapons, and related issues. Previously, he served as policy adviser to the secretary of defense’s representative for the new Strategic Arms Reduction Treaty, as an expert adviser to the Congressional Strategic Posture Commission, as a staff member on the President’s Commission on the Intdhgcnce Capa biLities of the US. Regarding WMD. and in a number of other government positions. Mr. Colby also serves or has served as a consultant to a number of U.S government bodies. He publishes and speaks regularly on strategic issues in the United States. Europe, and Asia. Mr. Colby is a graduate of Harvard College and Yale Law School and is a member of the Council on Foreign Rdations (term) and of the International Institute of Strategic Studies Abraham M. Denmark. cochair. is vice president for political and security affairs at the National Bure-au of Asian Research (NBR) and is an Asia-Pacific security adviser at the Center for Naval Analyses. He manages NBR research programs, dialogues, projects, and initiatives reLated to po. litical and security issues in the Asia-Pacific region. He has experience both inside and outside of government, having previously worked as a fellow at the Center for a New American Security and as country director for China affairs in the Office of the Secretary of Deknse. Mr. Denmark holds an MA. in international security from the Josef Korbel Schoel of International Studies at the University of Denver and has studied at China’s Foreign Atfairs University and Peking Universit, Nuclear Weapons and U.S.-China Relations, <http://csis.org/files/publication/130307_Colby_USChinaNuclear_Web.pdf>

Taiwan. **Taiwan remains the single most plausible and dangerous source of tension and conflict between the United States and China**. Beijing continues to be set on a policy to prevent Taiwan’s independence, and the United States maintains the capability to come to Taiwan’s defense. Although the tensions across the Taiwan Strait have subsided since both Taipei and Beijing embraced a policy of engagement in 2008, the situation remains combustible, complicated, by rapidly-diverging cross-strait military capabilities and persistent political disagreements. Moreover, for the foreseeable future Taiwan is the contingency in which **nuclear weapons would most likely become a major factor**, because the fate of the island is intertwined both with the legitimacy of the **C**hinese **C**ommunist **P**arty and the reliability of U.S. defense commitments in the Asia-Pacific region.

**So does conflict over the South China Sea**

**Rehman, 3/9, Stanton Nuclear Security Fellow**, Iskander Rehman was an associate in the Nuclear Policy Program at the Carnegie Endowment and a Stanton Nuclear Security Fellow. His research focuses on security and crisis stability in Asia, specifically the geopolitical ramifications of naval nuclearization in the Indian Ocean, 3/9/13, Dragon in a Bathtub: Chinese Nuclear Submarines and the South China Sea, <http://carnegieendowment.org/2013/03/09/dragon-in-bathtub-chinese-nuclear-submarines-and-south-china-sea/fpjl>

Despite America’s [best efforts to construct stronger ties with China](http://www.foreignaffairs.com/articles/64946/elizabeth-c-economy-and-adam-segal/the-g-2-mirage), relations in-between both countries have been repeatedly buffeted by a series of tensions and misunderstandings. Many of these frictions appear to have resulted from a more [assertive Chinese posture](http://nation.time.com/2012/07/15/the-south-china-sea-from-bad-to-worse/) in the South China Sea. Almost every week, Asian headlines seem to be dominated by reports of jingoistic statements over disputed islets, or of a renewed bout of aggressive maneuvering by boats from one of Beijings numerous maritime agencies. When attempting to explain this upsurge in Chinese pugnacity, analysts have pointed to the rising power's selective interpretation of the law of the sea and growing unwillingness to compromise over what it calls its [“blue national soil”](http://www.washingtonpost.com/opinions/the-blue-national-soil-of-chinas-navy/2011/03/18/AB5AxAs_story.html), particularly when confronted with an increasingly intransigent domestic populace. Others have pointed to the more immediately tangible benefits to be derived from the presence of [numerous offshore oil and gas deposits](http://thediplomat.com/2012/02/04/beijings-south-china-sea-gamble/) within contested waters.  Strangely enough, however, one of the principal explanations for China’s increased prickliness towards foreign military presence within its maritime backyard has yet to be clearly articulated.

Indeed, not only is the South China Sea one of the world’s busiest trade thoroughfares, it also happens to be the roaming pen of China’s emerging ballistic missile submarine fleet, which is stationed at [Sanya](http://www.fas.org/blog/ssp/2008/04/new-chinese-ssbn-deploys-to-hainan-island-naval-base.php), on the tropical Island of Hainan. The United States, with its array of advanced anti-submarine warfare assets and hydrographic research vessels deployed throughout the region, gives Beijing the unwelcome impression that Uncle Sam can’t stop peering into its nuclear nursery. When Chinese naval strategists discuss their maritime environs, the sentiment they convey is one of [perpetual embattlement](http://www.nytimes.com/2012/09/28/opinion/between-US-and-Asia-the-best-defense-is-dialogue.html?_r=0). Pointing to the US’s extended network of allies in the Indo-Pacific region, and to their own relative isolation, Chinese strategists fear that Beijing’s growing navy could be ensnared within the first island chain-a region which they describe as stretching from Japan all the way to the Indonesian archipelago.  Applying this maritime siege mentality to naval planning; they fret that the US Navy could locate and neutralize their fledgling undersea deterrent in the very first phases of conflict, before it even manages to slip through the chinks of first island chain.

This concern helps explain China's growing intolerance to foreign military activities in the South China Sea. Tellingly, some of the most nerve-wracking standoffs involving US and Chinese forces have unfolded in close proximity to Hainan. The infamous [Ep-3 crisis](http://news.bbc.co.uk/2/hi/asia-pacific/1260290.stm), during which a US spy plane entered into collision with a Chinese fighter jet, occurred while the plane’s crew was attempting to collect intelligence on naval infrastructure development. Similarly, the [USNS Impeccable incident](http://www.nytimes.com/2009/03/12/washington/12web-china.html), during which a US hydrographic vessel was dangerously harassed by five Chinese ships, took place approximately seventy miles to the south of Hainan. During the confrontation, Chinese sailors reportedly attempted to unhook the Impeccable’s towed acoustic array sonars.

In public, China's protests over foreign military activities are couched in territorial terms. In private, however, **Chinese policymakers readily acknowledge the centrality of the nuclear dimension**. Thus in the course of a discussion with a former Chinese official, I was told that “even though territorial issues are of importance, our major concern is the sanctity of our future sea-based deterrent.” He then went on to describe, with a flicker of amusement, how fishermen off the coast of Hainan regularly snag US sonars in their nets, and are encouraged to sell them back to the local authorities in exchange for financial compensation. Of course, such cat and mouse games are nothing new-and are perfectly legal- provided they occur within international waters or airspace. During the Cold War, American and Soviet ships would frequently conduct forward intelligence gathering missions, sometimes in very close proximity to each others’ shores. At the time, [American thinkers cautioned](http://books.google.com/books?hl=fr&lr=&id=rqnNaG2jL7wC&oi=fnd&pg=PR9&dq=barry+posen+inadvertent+escalation&ots=0esVgPTh4H&sig=maTUiyNXIx2Oo_eJFnvxIzPcf1M) that such risky behavior could potentially lead to misinterpretation and nuclear disaster. Unlike the Soviets, however, who could confine the movements of their boomers to the frigid, lonely waters of the Barents and Okhotsk seas, the Chinese have chosen to erect their nuclear submarine base smack-bang in the middle of one of the world’s busiest maritime highways.

Needless to say, this location is hardly ideal. When it comes to picking strategic real-estate in their near seas, the Chinese have but a limited roster of options. After all, their maritime backyard is girded by a sturdy palisade of states which increasingly view China’s meteoric rise, and attendant truculence at sea, with a mixture of alarm and dismay. Like a dragon caught floundering in a bathtub, China’s naval ambitions are simply too broad and grandiose for its constricted maritime geography. This perceived lack of strategic depth provides a partial explanation to Beijing’s increased obduracy over territorial disputes in the South China Sea. In order to better protect its valuable subsurface assets, China aims to establish a ring of maritime watch towers or bastions around Hainan. Absolute control over the remote [Spratly islands](http://hir.harvard.edu/the-spratly-islands-dispute-order-building-on-china-s-terms), in addition to the more proximate Paracels, would greatly facilitate this concentric defensive configuration.

Until not long ago, China’s strategic submarine force wasn’t really taken seriously. Their lone 0-92 Xia class boat was deemed too [antiquated](http://www.globalsecurity.org/wmd/world/china/type_92.htm)-and noisy-to be anything more than a symbol of Beijing’s desire for great power status. Some observers had ventured that China would be content to rely almost exclusively on its rapidly modernizing land-based missile system for its deterrent. Recent developments, however, suggest that this may be about to change. In its [latest report to Congress](http://www.reuters.com/article/2012/11/08/us-china-usa-military-idUSBRE8A705720121108), the US-China Economic and Security Review Commission stated that China could soon equip its new class of Jin submarines with the JL-2 ballistic missile, which has a range of approximately 4 600 miles. This would enable Beijing, the report adds, to establish a “near-continuous at-sea strategic deterrent”.  In all likelihood this force will be berthed at Hainan. The second Obama Administration will therefore have the unenviable task of dealing with tensions in a region which is not only riddled with territorial divisions, but is also **rapidly morphing into one of the world’s most sensitive nuclear hotspots.**

# 2AC

## 2AC AT: Strike China CP

**The impact is nuclear war**

**Plate 3** [Tom, Professor at UCLA, The Straights Times, “Neo-cons a bigger risk to Bush than China,” 6-28-2003]

But imagine a China disintegrating- on its own, without neo-conservative or Central Intelligence Agency prompting, much less outright military invasion because the economy (against all predictions) suddenly collapses. That would knock Asia into chaos. A massive flood of refugees would head for Indonesia and other places with poor border controls, which don’t’ want them and can’t handle them; some in Japan might lick their lips at the prospect of World War II revisited and look to annex a slice of China. That would send Singapore and Malaysia- once occupied by Japan- into nervous breakdowns. Meanwhile, India might make a grab for Tibet, and Pakistan for Kashmir. Then you can say hello to World War III, Asia style. That’s why wise policy encourages Chinese stability, security and economic growth – the very direction the White House now seems to prefer.

## 2AC AT: 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)

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.

**2AC AT: XO**

**It gets rolled back — also can’t solve legal norms**

**Swanson 9**, Chair of accountability and prosecution working group of United for Peace and Justice

(David, 1/25, Dangerous Executive Orders, www.opednews.com/articles/Dangerous-Executive-Orders-by-David-Swanson-090125-670.html)

The Center for Constitutional Rights has expressed concern that President Obama's executive order banning torture may contain a loophole. But **no president has any right to declare torture legal or illegal**, with or without loopholes. And **if we accept that presidents have such powers, even if our new president does good with them, then loopholes will be the least of our worries**. Torture is, and has long been, illegal in every case, without exception. It is banned by our Bill of Rights, the Universal Declaration of Human Rights, the Geneva Convention relative to the Treatment of Prisoners of War, the International Covenant on Civil and Political Rights, the Convention Against Torture and Other Cruel Inhuman or Degrading Treatment or Punishment, and Title 18, U.S. Code, Section 2340A. Nothing any president can do can change this or unchange it, weaken it or strengthen it in any way. Preventing torture does not require new legislation from Congress or new orders from a new president. It requires enforcing existing laws. In fact, adherence to the Convention Against Torture, which under Article VI of our Constitution is the supreme law of the land, requires the criminal prosecution of torturers and anyone complicit in torture. Most of the seemingly noble steps taken by Congress in recent years and by President Obama in his first week have served to disguise the fact that torture always was, still is, and shall continue to be illegal. In 2005, John McCain championed the McCain Detainee Amendment to the Defense Appropriations bill for 2005, which passed the Congress and was signed into law by President Bush. This was yet another law banning torture. It was not needed, but no harm done, right? Wrong. Passing laws like this serves to create the illusion that torture was previously legal. And that allows the new laws to create exceptions. In fact, McCain allowed a major loophole for the CIA. And that would have been bad enough. But President Bush tacked on a "signing statement" throwing out the entire ban on torture. So, with Congress trying to ban torture, and the president eliminating the ban, people could hardly be blamed for believing torture was legal. President **Bush** also **signed executive orders and ordered the creation of legal opinions claiming that torture was legal.** President **Obama's new order revokes one of Bush's. But Obama has no more right to undo the legalization of torture than Bush had to legalize it in the first place**. **Only Congress** has or **should have the power to legislate**. Obama's new order requires adherence to laws, rather than claiming the right to violate them, and yet there is a wide gap between publishing an order requiring adherence to the laws and actually enforcing the laws by indicting violators**. The same order that President Obama uses to ban torture also orders the closure of all CIA detention facilities**. Congress never authorized the creation of such things in the first place. Ordering their closure is the right thing to do. **But if a president can give the order to close them, what is to prevent another president giving the order to reopen them?** The answer should be all of the laws and treaties violated. Obama's executive order largely orders the government to cease violating various laws. But in so doing, **rather than strengthening the laws, the new president weakens them almost to the point of nonexistence**. For, what power does a law have to control behavior if it is never enforced? What deterrent value can be found in a law the violation of which results merely in a formal order to begin obeying it? And what status are we supposed to give all the other violated laws for which no such formal orders have been given?

**Perm — do both — Congressional involvement makes the plan popular — the CP links to politics**

**Corcoran 11** --- Professor of Law and Director at University of New Hampshire School of Law (March 2011, Erin M., University of New Hampshire Law Review, “Obama's Failed Attempt to Close Gitmo: Why Executive Orders Can't Bring About Systemic Change,” 9 U.N.H. L. Rev. 207))

Finally, this example highlights that **issuing unilateral executive orders, and then asking Congress to fund those decisions, is much less effective than having Congress help create the framework for significant policy changes.** Congress is an independent branch of government regardless of whether the members' party affiliation is the same as the President's. **Since members of the House are elected every two years, they are particularly sensitive to the idiosyncratic whims of the constituents in their district**. For the President, it is often easier to support sweeping change on a policy level. Although Senators are elected every six years, they are still bound to protect parochial concerns of their constituents. **Congress members go home every weekend to their respective districts and must explain their votes, decisions, and legislative priorities to the voters** often at supermarkets, churches, and bingo halls.

**Often times, when members of Congress can control the message or create the narrative addressing the problem, they can show their** [\*235] constituents **how their votes are in line with constituent priorities and concerns. In contrast, when Congress is told to do what the President wants and fund a controversial proposal, the members are in less control of the message and less invested in the outcome.**

Furthermore, in the Senate, particularly in the Appropriations Committee, members work across the aisle. Until recently, appropriators tended to vote as a block regardless of party affiliation, protecting their funding prerogatives and funding for their home districts. For example, the Senate Supplemental Appropriations mark included funding to close Guantanamo Bay. Yet, **during the Senate floor debate about closing Guantanamo Bay, ultimately it was the Chair of the Appropriations Committee who filed the amendment on the floor to strip funding out of the supplemental bill.** n150 **The Chair's action provided cover to other appropriators to vote in support of stripping the funding.** Since the Chair authored the amendment, there was no longer any obligation to support the appropriations bill as it was marked up out of committee. Generally, appropriators vote together to protect funding when other senators attempt to strip funding out of appropriations bills or move funds from one account to fund a priority not accommodated by the appropriators. **Since these members value collegiality, compromise, and consultation, it is no surprise that Obama's efforts to fund Guantanamo Bay closure was thwarted. If the Senate had been charged with crafting legislation, the members would have been committed to making sure they had the votes to pass it.**

Overall, if the Obama Administration wants to close Guantanamo Bay, it must get Congress to lead the charge. This is going to be extremely difficult now with a Republican House of Representatives and Democrat Senate that holds the majority by the narrowest of margins. At this point, it seems as if the Administration has abandoned its campaign to close Guantanamo Bay. The only silver lining is that the Administration hopefully has learned important lessons on what works and what is a non-starter and can use this knowledge when advancing the President's future controversial policy changes.

**Links to politics**

**Hallowell 13** writer for The Blaze, Here’s How Obama is Using Executive Power to Bypass Legislative Process, <http://www.theblaze.com/stories/2013/02/11/heres-how-obamas-using-executive-power-to-bylass-legislative-process-plus-a-brief-history-of-executive-orders/>

“In an era of polarized parties and a fragmented Congress, the opportunities to legislate are few and far between,” Howell said. “So presidents have powerful incentive to go it alone. And they do.”¶ **And the political opposition howls.**¶ Sen. Marco Rubio, R-Fla., a possible contender for the Republican presidential nomination in 2016, said that on the gun-control front in particular, Obama is “abusing his power by imposing his policies via executive fiat instead of allowing them to be debated in Congress.”¶ The Republican reaction is to be expected, said John Woolley, co-director of the American Presidency Project at the University of California in Santa Barbara.¶ “For years there has been a growing concern about unchecked executive power,” Woolley said. “It tends to have a partisan content, with contemporary complaints coming from the incumbent president’s opponents.”

**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.

**Russian cyber security stops nuclear war**

**Schaap 9, major stationed at the Directorate of Legal Services**

(Arie J., B.A., University of North Dakota (1995); J.D., California Western School of Law (1999); LL.M., George Washington University (2008), “CYBERLAW EDITION: CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW” Air Force Law Review 64 A.F. L. Rev. 121, Lexis)

As states begin to focus their energies on developing doctrine and weapons for conducting cyber warfare operations, it is essential that we move beyond just the realization that cyberspace is an important new battleground for conducting warfare operations and recognize the need to come to an understanding of what rules regulate this new battlefield. One commentator noted: The rapid advancement of cyber attacks and the emergence of cyber warfare have caught government [\*124] and military leaders around the world off guard. Decision making in time requiring defensive measures or military crisis is guided by doctrine and rules of engagement, but in the case of cyber attacks and cyber warfare they do not currently exist. n8 For over a century, states have developed rules of international law, such as the Geneva Conventions, which seek to avoid war or minimize human suffering when conflicts occur. n9 Additionally, as new technologies emerge, states have drafted new sets of laws, such as treaties restricting biological, chemical and laser weapons. n10 Yet governments have so far resisted calls to craft new rules of international law to govern attacks on or by computers. n11 As a result, current international law does not explicitly address cyber warfare. n12 However, the fact that a particular military activity is not specifically regulated does not mean it can be used without restrictions. n13 While the international community remains unsettled on whether cyber techniques are legally considered weapons and whether cyber attacks can be considered legitimate acts of armed conflict, n14 the **denial of service** (DoS) **attacks** against Estonia in 2007 and Georgia in 2008 **illustrate** that this **new form of warfare is operational** **and** also **reinforces the need to develop** a better understanding of how **international law** relates to cyber warfare. Without such an understanding, **this emerging form of warfare will create uncertainties** **as to the legality** **of** certain **acts**; this uncertainty **has the potential to then escalate tensions and intensify military operations** beyond the cyber domain. For example, **more than one senior Russian military official supported the notion that "the use of Information Warfare against Russia** or its armed forces **will** categorically **not be considered** a **non-military** phase of a conflict whether there were casualties or not" n15 and that "**Russia retains the righ**t [\*125] **to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor State itself."** n16

## 2AC AT: Cyber Deterrence DA

#### 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>

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.

=MARKED=

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.**

## 2AC AT: Flexibility DA

#### Turn — oversight requirement creates greater executive knowledge of operations — that’s Lorber — more ev

**NRC 9**, WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP Staff HERBERT S. LIN, Study Director KRISTEN BATCH, Associate Staff Officer (through August 2008) TED SCHMITT, Consultant JANICE SABUDA, Senior Project Assistant (through March 2008) ERIC WHITAKER, Senior Project Assistant JOSEPH F. TRAUB, Columbia University, Chair PRITHVIRAJ BANERJEE, Hewlett Packard Company FREDERICK R. CHANG, University of Texas, Austin WILLIAM DALLY, Stanford University MARK E. DEAN, IBM Almaden Research Center DEBORAH L. ESTRIN, University of California, Los Angeles KEVIN C. KAHN, Intel Corporation JAMES KAJIYA, Microsoft Corporation RANDY H. KATZ, University of California, Berkeley JOHN E. KELLY III, IBM Research SARA KIESLER, Carnegie Mellon University JON KLEINBERG, Cornell University PETER LEE, Carnegie Mellon University TERESA H. MENG, Stanford University WILLIAM H. PRESS, University of Texas, Austin PRABHAKAR RAGHAVAN, Yahoo! Research DAVID E. SHAW, D.E. Shaw Research ALFRED Z. SPECTOR, Google, Inc. ROBERT F. SPROULL, Sun Microsystems, Inc. PETER SZOLOVITS, Massachusetts Institute of Technology ANDREW J. VITERBI, Viterbi Group, LLC PETER WEINBERGER, Google, Inc. JON EISENBERG, Director RENEE HAWKINS, Financial and Administrative Manager HERBERT S. LIN, Chief Scientist, CSTB LYNETTE I. MILLETT, Senior Program Officer NANCY GILLIS, Program Officer

ENITAA. WILLIAMS, Associate Program Officer MORGAN R. MOTTO, Program Associate SHENAE BRADLEY, Senior Program Assistant ERIC WHITAKER, Senior Program Assistant, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of CYBERATTACK CAPABILITIES, <http://www.anagram.com/berson/nrcoiw.pdf>

Recommendation 5: The U.S. government should provide a periodic accounting of cyberattacks undertaken by the U.S. armed forces, federal law enforcement agencies, intelligence agencies, and any other agencies with authorities to conduct such attacks in sufficient detail to provide decision makers with a more comprehensive understanding of these activities. Such an accounting should be made available both to senior decision makers in the executive branch and to the appropriate congressional leaders and committees. Whether or not cyberattack falls into the category of covert action, it appears that even within the executive branch, knowledge of the actual cyberattack activities of the United States is **highly fragmented**. An authoritative source, updated periodically, that documents the extent and nature of such activities and provides analyses of their impact and/ or significance would help senior decision makers within the executive branch and Congress in carrying out their authorization and oversight responsibilities.

#### Turn — the aff fosters external review and coordination — that increases effectiveness

**NRC 9**, WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP Staff HERBERT S. LIN, Study Director KRISTEN BATCH, Associate Staff Officer (through August 2008) TED SCHMITT, Consultant JANICE SABUDA, Senior Project Assistant (through March 2008) ERIC WHITAKER, Senior Project Assistant JOSEPH F. TRAUB, Columbia University, Chair PRITHVIRAJ BANERJEE, Hewlett Packard Company FREDERICK R. CHANG, University of Texas, Austin WILLIAM DALLY, Stanford University MARK E. DEAN, IBM Almaden Research Center DEBORAH L. ESTRIN, University of California, Los Angeles KEVIN C. KAHN, Intel Corporation JAMES KAJIYA, Microsoft Corporation RANDY H. KATZ, University of California, Berkeley JOHN E. KELLY III, IBM Research SARA KIESLER, Carnegie Mellon University JON KLEINBERG, Cornell University PETER LEE, Carnegie Mellon University TERESA H. MENG, Stanford University WILLIAM H. PRESS, University of Texas, Austin PRABHAKAR RAGHAVAN, Yahoo! Research DAVID E. SHAW, D.E. Shaw Research ALFRED Z. SPECTOR, Google, Inc. ROBERT F. SPROULL, Sun Microsystems, Inc. PETER SZOLOVITS, Massachusetts Institute of Technology ANDREW J. VITERBI, Viterbi Group, LLC PETER WEINBERGER, Google, Inc. JON EISENBERG, Director RENEE HAWKINS, Financial and Administrative Manager HERBERT S. LIN, Chief Scientist, CSTB LYNETTE I. MILLETT, Senior Program Officer NANCY GILLIS, Program Officer

ENITAA. WILLIAMS, Associate Program Officer MORGAN R. MOTTO, Program Associate SHENAE BRADLEY, Senior Program Assistant ERIC WHITAKER, Senior Program Assistant, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of CYBERATTACK CAPABILITIES, <http://www.anagram.com/berson/nrcoiw.pdf>

As an example of a question for which the U.S. government as a whole needs to establish an authoritative decision-making structure, consider cyberattack in the context of the dividing line between covert action and military activity. The U.S. Code defines covert action as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly” (50 USC 413b(e)). At the same time, the U.S. code also defines any activity executed under control of the DOD chain of command as falling under the definition of a traditional military activity associated with anticipated or ongoing hostilities, and such activity thus is not covert action subject to the findings and congressional reporting process. The question of the boundaries between covert action and traditional military activities has been the subject of much discussion over the past several years (since the U.S. invasions of Afghanistan and Iraq). The findings and reporting process is often disliked by incumbent administrations, because it constrains an administration’s ability to act freely and quickly and runs the risk of leaks that may reveal the existence of a covert action. On the other hand, many informed advocates of the process believe that the existence of such a process forces the executive branch to coordinate internal stakeholders and their equities, and also provides for necessary external review of actions that may be ill-advised from a broader public policy perspective.

#### 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.

Clarify Authorization and Accountability for Cyberoperations. Operations in cyberspace tend to defy categorization by type (collection, covert action, or military activity) or geographic location. This causes problems on all the dimensions mentioned above, while also raising difficult questions regarding when an agency has the affirmative authority to conduct such operations in the first place. Legislation can resolve much of this uncertainty by (i) clarifying that the military has standing authority to conduct computer network attacks (unacknowledged or otherwise) when acting in a defensive capacity or under color of a statutory authorization for the use of military force, and (ii) providing timely notification to the House and Senate Armed Services Committees of such operations when they have or are likely to have significant consequences outside a theater of combat operations.

## 2AC AT: Politics (DC) --- UMKC

**Partisan fights mean it won’t pass**

**Weisman, 9-12**-’13 (Jonathan, “Boehner Seeking Democrats’ Help on Fiscal Talks” http://www.nytimes.com/2013/09/13/us/politics/at-meeting-with-treasury-secretary-boehner-pressed-for-debt-ceiling-deal.html?pagewanted=all)

Much of the federal government will shut down as of Oct. 1 unless Congress approves new spending bills to replace expiring ones, and by mid-October, the Treasury Department will lose the borrowing authority to finance the government and pay its debts. **“It’s time for the president’s party to** show the courage to **work with us to solve this problem,” said** Mr. **Boehner**, who argued that budget deals have been part of past agreements to raise the debt limit **But** a bloc of **43 House Republicans undercut the speaker’s deficit-reduction focus, introducing yearlong funding legislation that would increase Pentagon and veterans spending and delay** President Obama’s **health care** law for a year — most likely adding to the budget deficit. **That bloc is large enough to thwart any compromise that does not attract Democratic support**. “Obamacare is the most dangerous piece of legislation ever passed in Congress,” said Representative John Fleming, Republican of Louisiana. “It is the most existential threat to our economy” that the country has seen “since the Great Depression, so I think a little bit of additional deficit is nothing,” he added. **Just five** scheduled **legislative days stand between the House and a government shutdown** that has loomed for months. As of now, **Republican leaders appear to have no idea how to stop it**. House members are preparing for the worst. A 14-page fact sheet on the impact of a government shutdown, originally written in 2011 by Representative Scott Rigell, Republican of Virginia, has gone back into circulation among House members. Mr. Lew and Congressional **Democrats held firm that they would no longer negotiate on raising the debt ceiling**, which they see as the duty of the party in power in the House. And **they made it clear** to the speaker that **they would never accept Republican demands to repeal, defund or delay** Mr. Obama’s signature **health care** law. **White House officials dismissed it as “a nonstarter**.” “I had to be very candid with him and I told him directly, all these things they’re doing on Obamacare are just a waste of their time,” said Senator Harry Reid, Democrat of Nevada and the Senate majority leader. “Their direction is the direction toward shutting down the government.” “I like John Boehner,” Mr. Reid added. “I do feel sorry for him.”

#### Turn — the plan’s bipartisan

**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.

#### Syria thumps

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))

President Obama may have avoided an embarrassing legislative defeat over Syria, but the debate left him weakened at a critical point in his second term, according to GOP and Democratic insiders on Capitol Hill.

In a whirlwind period for both the White House and Congress, Obama pressed for an immediate military attack against Syria before eventually asking lawmakers to delay a vote authorizing the use of force to pursue a Russian-backed diplomatic solution.

Obama’s push to punish Syrian leader Bashar Assad for using chemical weapons faced stiff opposition from both lawmakers and the public and cost him in the polls.

Many on Capitol Hill say Obama squandered momentum that could have been better served on key challenges ahead.

Obama faces crucial fights over funding the federal government, raising the nation’s debt limit, turning off the next round of sequester cuts, rolling out his healthcare reforms and overhauling the nation’s immigration laws.

“It’s certainly true that [Obama] used up a lot of political capital, apparently for nothing, on the authorization push,” a senior House GOP leadership aide told the Washington Examiner.

The aide added that the Syrian standoff could still cost the president further leverage.

Secretary of State John Kerry is to begin talks with his Russian counterpart Wednesday on a plan to have Damascus turn over its chemical weapons to international inspectors, but the prospects for a deal are uncertain.

White House press secretary Jay Carney on Wednesday declined to lay out a timeline for talks, saying only that it would “take some time.”

"I think the bigger effect is still not known,” said the GOP aide. “If somehow the Russians do help get rid of the [Syrian] regime’s chemical weapons, the president will come out fine. But if Putin and Assad just toy with him for the next month, there’s no doubt he will have an exceedingly weakened presidency and ability to make demands of anyone.”

National security analysts say it would be virtually impossible to ensure Assad turns over his chemical weapons amid the country’s brutal civil war. And even some White House officials have privately questioned whether they are being played by Russian President Vladimir Putin’s offer to help facilitate the destruction of Syria’s chemical arsenal.

An adviser to a high-ranking Democratic senator with close ties to Obama conceded that Syria could remain a distraction as the president turns his attention to his domestic agenda.

“It doesn’t make the president’s job this fall any easier,” the aide said. “There’s not a whole lot for us to rally around at this point. Obviously, it’s not the boost the White House had hoped for.”

“Do I fear a carryover effect?” the source added. “I do.”

#### And the budget

Sink, 9/12 (Justin, 9/12/2013, “White House: President will reject ObamaCare defunding measure,” <http://thehill.com/blogs/blog-briefing-room/news/322017-white-house-obama-open-to-approving-resolution-to-prevent-shutdown>)

The White House has suggested in recent days that they are returning their focus to the budget after the crisis in Syria dominated attention in recent weeks. Obama will visit leaders at the Business Roundtable next week — a forum he has used before to press lawmakers to strike a budget deal.

Earlier Thursday, Obama said that the American people remained interested in lawmakers "dealing properly with a federal budget, that bills are being paid on time, that the full faith and credit of the United States is preserved and that the federal government itself, in every single agency, is running the way it should, making sure that our constituents, the American people, are getting good service."

#### And CIR

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.

#### And Obama’s being blasted on war powers

Nelson, 9/5 (Colleen, 9/5/2013, “Obama's Curbs on Executive Power Draw Fire,” <http://online.wsj.com/article/SB10001424127887323893004579057463262293446.html>))

President Barack Obama, who pledged to push his second-term domestic agenda through executive actions when Congress wouldn't cooperate, has moved in the opposite direction on international affairs in recent months as he created new checks on executive authority.

By asking Congress to authorize military action against Syria, proposing some constraints on National Security Agency surveillance programs and placing limits on drone strikes, the president voluntarily has ceded some authority in foreign policy and national security, legal experts say.

The president's moves on national-security issues reflect a mix of political pragmatism as well as personal principles, and exactly how much power Mr. Obama actually has given up is the subject of debate. He has walked a fine line on Syria, for example, saying he wasn't required to seek sign-off from lawmakers for a military strike but asking for their approval anyway.

A senior administration official said that while the new drone-strike policy does rein in executive authority, the NSA and Syria proposals weren't a reduction of power but an effort to increase transparency and build public confidence.

Still, the president, who was criticized for seizing too much power through recess appointments and other steps that some said circumvented Congress, now is being criticized by veterans of past Republican administrations for weakening the presidency.

John Yoo, a Justice Department official in the George W. Bush administration, said Mr. Obama had unnecessarily limited his own authority. He noted that it is rare to see a president restrict his powers.

Mr. Obama "has been trying to reduce the discretion of the president when it comes to national security and foreign affairs," said Mr. Yoo, now a law professor at the University of California at Berkeley. "These proposals that President Obama is making really run counter to why we have a president and a constitution."

#### The plan’s not perceived

**Schmitt 13**, **co-director of the Marilyn Ware Center for Security Studies at AEI** and the director of AEI's Program on American Citizenship. Mr. Schmitt is a former staff director of the Senate Select Committee on Intelligence. He was executive director of the President's Foreign Intelligence Advisory Board during President Ronald Reagan's second term. Mr. Schmitt's security work focuses on longer-term strategic issues that will affect America's security at home and its ability to lead abroad, while his work in the area of citizenship focuses on challenges to maintaining and sustaining a strong civic culture. His books include Of Men and Materiel: The Crisis in Military Resources (AEI Press, 2007), to which he was a contributing author and editor with Tom Donnelly; Silent Warfare: Understanding the World of Intelligence (Brassey’s, 2002), coauthored with Abram Shulsky and now in its third edition; and U.S. Intelligence at the Crossroads: Agendas for Reform (Brassey’s, 1995), a coedited volume to which he is a contributing author. His two most recent books, to which he is also editor and contributing author, are The Rise of China: Essays on the Future Competition (Encounter Books, May 2009) and Safety, Liberty and Islamist Terrorism: American and European Approaches to Domestic Counterterrorism (AEI Press, 2010), <http://www.aei-ideas.org/2011/12/authorization-for-cyber-attacks/>

The press (and the White House) has been obsessed by the detention provision in the recently agreed upon FY2012 Defense Authorization bill, but one of the items that **slipped under the radar** is language authorizing the American military to engage in offensive operations in cyberspace. Under Sec. 954,

Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, allies and interests.

**Obama not negotiating over debt ceiling**

**Pianin, 9/10** (Eric, 9/10/2013, “Debt-Ceiling Danger Zone Threatens U.S.,” <http://www.thefiscaltimes.com/Articles/2013/09/10/Debt-Ceiling-Danger-Zone-Threatens-US>))

Once that threshold is crossed, the government could default on payments to major creditors, begin shuttering federal agencies, furloughing workers or miss making Social Security payments to retirees. **Obama has repeatedly said there will be no political bargaining over the debt ceiling, as there was two years ago**. However, **the top four Democratic and Republican leaders will meet privately on Thursday to discuss the debt ceiling and how to avoid a government shutdown before Oct 1**, according to Politico.

The meeting, requested by Senate Majority Leader Harry Reid (D-NV), will be the first time the group has met since they departed Washington for the August recess. **It will include** House Speaker John **Boehner** (R-OH), House Minority Leader Nancy **Pelosi** (D-CA) **and** Senate Minority Leader Mitch **McConnell** (R-KY).

Boehner said recently he’s gearing up for “a whale of a fight” with Obama over raising the debt ceiling, and that he’ll demand major concessions in terms of spending cuts and entitlement reforms in return for increasing the government’s nearly $16.7 trillion of borrowing authority. It would take an additional $1.1 trillion of borrowing authority to get the government through 2014, according to BPC’s analysis.

#### **Pol cap fails**

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))

The Syria debate highlighted tensions between the president and Democratic lawmakers, with many of his party’s most liberal members failing to rally behind him in the foreign policy debate. Even many from both parties who backed him on Syria suggested the president had poorly managed the effort to sway congressional support. Rep. Adam Kinzinger, R-Ill., said he had offered to help the White House rally support on Syria and never heard back. Many on both sides of the aisle now wonder how Obama will refine his effort to reach out to lawmakers in the domestic fights ahead. White House officials have long scoffed at the notion that Obama could enhance his political clout by fostering better personal relationships with lawmakers. They say that a round of golf, dinner diplomacy or extensive presidential backslapping will do little to help push the president’s agenda in the GOP-controlled House.But if Obama’s muddled Syria message proved anything, it’s that that he still doesn’t have the level of pull needed on Capitol Hill to force skittish Democrats to get in line or reachable Republicans to buck their party base. Carney on Wednesday sidestepped questions about whether the Syria debate had weakened Obama’s standing. “I'm not going to make a political assessment," he said. Time is working against White House efforts to regain any leverage, though. Congress has just six working days left in September to pass a continuing resolution to keep the government funded. That will coincide with the government reaching its borrowing capacity in October and a possible default on its debt. The White House is banking that Republican infighting over government funding will aid their cause. House leadership is pushing back a vote on keeping the government funded until next week. Many conservative lawmakers and outside groups want to use the bill to defund Obamacare. House GOP leaders, though, are trying to win votes for a plan that would fund the government through mid-December, forcing the Senate to vote first on cutting money for healthcare reform.

#### Cyber-attacks destroy critical infrastructure — that devastates the economy

**Popular Mechanics 9** (Glenn Derene, “How Vulnerable is U.S. Infrastructure to a Major Cyber-Attack?”, Popular Mechanics, 10/1/09, [http://www.popularmechanics.com/technology/military/4307521)//JY](http://www.popularmechanics.com/technology/military/4307521%29//JY)

The next world war might not start with a bang, but with a blackout. An enemy could send a few lines of code to control computers at key power plants, causing equipment to overheat and melt down, plunging sectors of the U.S. and Canadian grid into darkness. Trains could roll to a stop on their tracks, while airport landing lights wink out and the few traffic lights that remain active blink at random. In the silence and darkness, citizens may panic, or they may just sit tight and wait for it all to reboot. Either way, much of the country would be blind and unresponsive to outside events. And that might be the enemy's objective: Divert America's attention while mounting an offensive against another country. Pentagon planners have long understood the danger of cyber attacks on U.S. military networks. Indeed, the Defense Department's Global Information Grid is one of the most frequently targeted computer networks on Earth. But the cat-and-mouse game of information espionage on military networks is not the only digital threat that keeps national-security experts up at night. There is a growing concern over the vulnerability of far more tangible assets essential to the economy and well-being of American citizens. Much of the critical infrastructure that **keeps the country humming**--water-treatment facilities, refineries, pipelines, dams, the electrical grid--is operated using a hodgepodge of technologies known as industrial control systems. Like banks and telecommunications networks, which are also generally considered critical infrastructure, these industrial facilities and utilities are owned by private companies that are responsible for maintaining their own security. But many of the control systems in the industrial world were installed years ago with few or no cyber-security features. That wasn't a big problem when these systems were self-contained. But in the past two decades, many of these controls have been patched into company computer networks, which are themselves linked to the Internet. And when it comes to computer security, a good rule of thumb is that any device that is computer-controlled and networked is vulnerable to hacking. Bad-guy hackers pulling the plug on public utilities is a common theme of Hollywood films, including 2007's Live Free or Die Hard, but such scenarios present more than a mere fictional scare to U.S. intelligence officials. According to Melissa Hathaway, cyber-coordination executive for the Office of the Director of National Intelligence, the list of potential adversaries in a cyber attack is long, ranging from disgruntled employees to criminals to hostile nations. Most experts agree that China and Russia routinely probe our industrial networks, looking for information and vulnerabilities to use as leverage in any potential dispute. James Lewis, a cyber-security expert for the policy think tank Center for Strategic and International Studies (CSIS), says that although cyber warfare couldn't cripple the U.S., it could serve as an effective military tactic. "If I were China, and I were going to invade Taiwan," he says, "and I needed to complete the conquest in seven days, then it's an attractive option to turn off all the electricity, screw up the banks and so on." Could the entire U.S. grid be taken down in such an attack? "The honest answer is that we don't know," Lewis says. "And I don't like that answer." Ghosts in the Machine In January 2008, senior CIA analyst Tom Donahue dropped a bombshell on a small conference of government officials and power-company engineers from the U.S. and Europe. He told them that extortionists had managed to hack into utilities in multiple regions outside the United States and disrupt power equipment. "In at least one case," he said, "the disruption caused a power outage affecting multiple cities." The CIA has been highly secretive about the incident, and Donahue would not discuss where the blackouts occurred or what companies were affected. But he admitted that the CIA had no idea who had perpetrated the attacks. Hackers had shaken down a public utility, it seems, and had gotten away with it. Some security professionals think that government officials have been guilty of as much drama-mongering on the issue as Hollywood has. "Honestly, I think the threat is overblown," says Bruce Schneier, author of Schneier on Security. "The risks today are due more to errors than to malicious intent." He sees Donahue's story as nothing more than a tenebrous rumor. Nevertheless, Schneier thinks vulnerabilities in infrastructure will eventually become a real national-security threat. The problem is that the errors that Schneier refers to can cause bad things to happen. Much of computer hacking is predicated on exploiting glitches in commonly used systems. Such exploits on a Windows PC are irritating, but at a nuclear facility, they can be unnerving. In August 2006, a glitch shut down the Browns Ferry nuclear power plant in northern Alabama. Plant administrators lost control of recirculation pumps on one of the plant's reactors because of excessive data traffic on the control-system network. The plant was forced to go offline temporarily. Nuclear plants are designed to shut down in the event of major malfunctions to prevent a Chernobyl-style catastrophe. But they also generate almost 20 percent of U.S. power. What if a hacker exploited a coding error in a cooling system to shut down a sizable piece of the nation's power supply? Incidents of digital malfunctions that cause danger to human life are rare, but such events have happened. In June 1999, in Bellingham, Wash., shortly before a routine delivery of gasoline by the Olympic Pipe Line Co., a worker updated a database for the company's pipeline computer-control system. According to a report by the National Transportation Safety Board, a simple typo in the database caused the system to fail, disabling remote control for the pipeline's operators, 98 miles away in Renton, Wash. Pressure began to build in the line, so the operator issued a command to open a secondary pump to relieve it, but the system was unresponsive. A weak point in the pipeline ruptured, releasing 237,000 gal of gasoline into nearby Whatcom Creek. An hour and a half later, the gasoline ignited. The ensuing fireball scorched more than a mile of riverbank, killing three people, including two 10-year-old boys, and damaged the city's water-treatment facility. Read more: How Vulnerable is U.S. Infrastructure to a Major Cyber Attack? - Popular Mechanics

#### Economic decline doesn’t cause war

Zakaria Editor Newsweek ‘9

(Fareed-, Dec. 12, Newsweek, “The Secrets of Stability”, http://www.newsweek.com/id/226425/page/1; Jacob)

One year ago, the world seemed as if it might be coming apart. The global financial system, which had fueled a great expansion of capitalism and trade across the world, was crumbling. All the certainties of the age of globalization—about the virtues of free markets, trade, and technology—were being called into question. Faith in the American model had collapsed. The financial industry had crumbled. Once-roaring emerging markets like China, India, and Brazil were sinking. Worldwide trade was shrinking to a degree not seen since the 1930s.

Pundits whose bearishness had been vindicated predicted we were doomed to a long, painful bust, with cascading failures in sector after sector, country after country. In a widely cited essay that appeared in The Atlantic this May, Simon Johnson, former chief economist of the International Monetary Fund, wrote: "The conventional wisdom among the elite is still that the current slump 'cannot be as bad as the Great Depression.' This view is wrong. What we face now could, in fact, be worse than the Great Depression."

Others predicted that these economic shocks would lead to political instability and violence in the worst-hit countries. At his confirmation hearing in February, the new U.S. director of national intelligence, Adm. Dennis Blair, cautioned the Senate that "the financial crisis and global recession are likely to produce a wave of economic crises in emerging-market nations over the next year." Hillary Clinton endorsed this grim view. And she was hardly alone. Foreign Policy ran a cover story predicting serious unrest in several emerging markets.

Of one thing everyone was sure: nothing would ever be the same again. Not the financial industry, not capitalism, not globalization.

One year later, how much has the world really changed? Well, Wall Street is home to two fewer investment banks (three, if you count Merrill Lynch). Some regional banks have gone bust. There was some turmoil in Moldova and (entirely unrelated to the financial crisis) in Iran. Severe problems remain, like high unemployment in the West, and we face new problems caused by responses to the crisis—soaring debt and fears of inflation. But overall, things look nothing like they did in the 1930s. The predictions of economic and political collapse have not materialized at all.

A key measure of fear and fragility is the ability of poor and unstable countries to borrow money on the debt markets. So consider this: the sovereign bonds of tottering Pakistan have returned 168 percent so far this year. All this doesn't add up to a recovery yet, but it does reflect a return to some level of normalcy. And that rebound has been so rapid that even the shrewdest observers remain puzzled. "The question I have at the back of my head is 'Is that it?' " says Charles Kaye, the co-head of Warburg Pincus. "We had this huge crisis, and now we're back to business as usual?"

This revival did not happen because markets managed to stabilize themselves on their own. Rather, governments, having learned the lessons of the Great Depression, were determined not to repeat the same mistakes once this crisis hit. By massively expanding state support for the economy—through central banks and national treasuries—they buffered the worst of the damage. (Whether they made new mistakes in the process remains to be seen.) The extensive social safety nets that have been established across the industrialized world also cushioned the pain felt by many. Times are still tough, but things are nowhere near as bad as in the 1930s, when governments played a tiny role in national economies.

It's true that the massive state interventions of the past year may be fueling some new bubbles: the cheap cash and government guarantees provided to banks, companies, and consumers have fueled some irrational exuberance in stock and bond markets. Yet these rallies also demonstrate the return of confidence, and confidence is a very powerful economic force. When John Maynard Keynes described his own prescriptions for economic growth, he believed government action could provide only a temporary fix until the real motor of the economy started cranking again—the animal spirits of investors, consumers, and companies seeking risk and profit.

Beyond all this, though, I believe there's a fundamental reason why we have not faced global collapse in the last year. It is the same reason that we weathered the stock-market crash of 1987, the recession of 1992, the Asian crisis of 1997, the Russian default of 1998, and the tech-bubble collapse of 2000. The current global economic system is inherently more resilient than we think. The world today is characterized by three major forces for stability, each reinforcing the other and each historical in nature.

The first is the spread of great-power peace. Since the end of the Cold War, the world's major powers have not competed with each other in geomilitary terms. There have been some political tensions, but measured by historical standards the globe today is stunningly free of friction between the mightiest nations. This lack of conflict is extremely rare in history. You would have to go back at least 175 years, if not 400, to find any prolonged period like the one we are living in. The number of people who have died as a result of wars, civil conflicts, and terrorism over the last 30 years has declined sharply (despite what you might think on the basis of overhyped fears about terrorism). And no wonder—three decades ago, the Soviet Union was still funding militias, governments, and guerrillas in dozens of countries around the world. And the United States was backing the other side in every one of those places. That clash of superpower proxies caused enormous bloodshed and instability: recall that 3 million people died in Indochina alone during the 1970s. Nothing like that is happening today.

Peace is like oxygen, Harvard's Joseph Nye has written. When you don't have it, it's all you can think about, but when you do, you don't appreciate your good fortune. Peace allows for the possibility of a stable economic life and trade. The peace that flowed from the end of the Cold War had a much larger effect because it was accompanied by the discrediting of socialism. The world was left with a sole superpower but also a single workable economic model—capitalism—albeit with many variants from Sweden to Hong Kong.

This consensus enabled the expansion of the global economy; in fact, it created for the first time a single world economy in which almost all countries across the globe were participants. That means everyone is invested in the same system. Today, while the nations of Eastern Europe might face an economic crisis, no one is suggesting that they abandon free-market capitalism and return to communism. In fact, around the world you see the opposite: even in the midst of this downturn, there have been few successful electoral appeals for a turn to socialism or a rejection of the current framework of political economy. Center-right parties have instead prospered in recent elections throughout the West.

The second force for stability is the victory—after a decades-long struggle—over the cancer of inflation. Thirty-five years ago, much of the world was plagued by high inflation, with deep social and political consequences. Severe inflation can be far more disruptive than a recession, because while recessions rob you of better jobs and wages that you might have had in the future, inflation robs you of what you have now by destroying your savings. In many countries in the 1970s, hyperinflation led to the destruction of the middle class, which was the background condition for many of the political dramas of the era—coups in Latin America, the suspension of democracy in India, the overthrow of the shah in Iran. But then in 1979, the tide began to turn when Paul Volcker took over the U.S. Federal Reserve and waged war against inflation. Over two decades, central banks managed to decisively beat down the beast. At this point, only one country in the world suffers from -hyperinflation: Zimbabwe. Low inflation allows people, businesses, and governments to plan for the future, a key precondition for stability.

Political and economic stability have each reinforced the other. And the third force that has underpinned the resilience of the global system is technological connectivity. Globalization has always existed in a sense in the modern world, but until recently its contours were mostly limited to trade: countries made goods and sold them abroad. Today the information revolution has created a much more deeply connected global system.

Managers in Arkansas can work with suppliers in Beijing on a real-time basis. The production of almost every complex manufactured product now involves input from a dozen countries in a tight global supply chain. And the consequences of connectivity go well beyond economics. Women in rural India have learned through satellite television about the independence of women in more modern countries. Citizens in Iran have used cell phones and the Internet to connect to their well-wishers beyond their borders. Globalization today is fundamentally about knowledge being dispersed across our world.

This diffusion of knowledge may actually be the most important reason for the stability of the current system. The majority of the world's nations have learned some basic lessons about political well-being and wealth creation. They have taken advantage of the opportunities provided by peace, low inflation, and technology to plug in to the global system. And they have seen the indisputable results. Despite all the turmoil of the past year, it's important to remember that more people have been lifted out of poverty over the last two decades than in the preceding 10. Clear-thinking citizens around the world are determined not to lose these gains by falling for some ideological chimera, or searching for a worker's utopia. They are even cautious about the appeals of hypernationalism and war. Most have been there, done that. And they know the price.