# 1AC

### 1AC Plan

#### The United States federal government should substantially increase statutory restrictions on the war powers authority of the President of the United States to prohibit the use of offensive cyber operations.

### 1ac -- Preemption

#### The Advantage is Preemption

**The US is militarizing cyberspace now -- congress needs to develop guide-lines and open discussion to the public**

**Romm 12/24** -- Tony Romm is a technology reporter for POLITICO Pro. He closely follows tech topics and debates on Capitol Hill and before agencies like the Federal Trade Commission, keeping a close eye on issues such as online privacy, antitrust and competitiveness, tech industry lobbying and PAC spending, intellectual property and cybersecurity. Romm has previously worked as a tech and general assignment blogger at The Hill, and his writing has appeared in publications such as The Washington Post, Slate and Stateline.org (Tony, "Pentagon's Cyber Arm Poised to Expand Role," politico.com, December 24, 2013, http://www.politico.com/story/2013/12/pentagon-cybersecurity-role-101485.html#ixzz2pIGwSc5x)

The U.S. military’s Cyber Command is about to receive the digital equivalent of faster ships and stronger missiles — **but the force**, only a few years in the making, **is still grappling with how far it can go in fighting adversaries in cyberspace.**

As part of the defense policy bill that just passed Congress, the Pentagon’s many cybersecurity initiatives together secured billions of dollars in funding as well as new resources to help train Cyber Command’s programmers and prepare them to operate on the emerging digital battlefield.
But the infusion comes as **CyberCom,** as it’s known, **is still working out** its fundamental **rules of engagement, including thorny questions as to when it can strike** back at hackers and whether it can act without getting approval from the president. It’s also struggling to find and train the talent it needs to carry out its mission, partly because of Pentagon budget pressures.

And CyberCom has become ensnared in the debate over National Security Agency surveillance sparked by Edward Snowden’s leaks. The cyber force shares a director and headquarters with the controversial spy agency — and some in Congress want to look at splitting the two operations.

It all points to growing pains — and more scrutiny — as CyberCom takes on a larger role in protecting the U.S. from attacks. Started chiefly to protect the Department of Defense’s own networks, the organization has morphed into an operation that seeks a much broader mandate to confront digital spies and hackers.

The command’s goal is to be “highly standardized, highly skilled, competent across the spectrum of conflict — high bars to prove the individual, the team, the force are trained and ready. Never been done before in cyber, but absolutely necessary,” said Maj. Gen. Brett Williams, director of operations with CyberCom, during a rare interview at its headquarters in Fort Meade, Md.

Cyber Command became fully operational in November 2010 after years of lobbying by Pentagon brass, and Gen. Keith Alexander has held its reins from the start. Defense leaders early on stressed that CyberCom’s role was to defend military networks “already under attack” and emphasized the goal wasn’t a “militarization” of cyberspace. But the operation has since grown in size and scope **to meet new threats emerging in China, Iran and beyond. Now, CyberCom boasts offensive** and defensive teams and runs regular exercises to prepare for worst-case scenarios. And **as it bulks up, Congress is working to give it additional tools**.

For example, the annual defense bill — approved last week by the Senate after earlier passing the House — **included a litany of initiatives that will benefit CyberCom, including $68 million for some of the operation’s classified activities**, more than $14 million for Air Force offensive cybersecurity work and a series of programs that could augment DOD’s ability to strike in cyberspace.

There’s $33 million set aside to help map the Internet, an effort that could allow CyberCom to better target digital foes. A project called Plan X under the military’s research hub, the Defense Advanced Research Projects Agency — **aimed at making cyber weaponry easier to deploy in the field — is getting a $2.5 million increase to speed up development. And CyberCom would get the nod to upgrade so-called cyber ranges, which essentially serve as private arenas for the military to train new cyber workers and test out its offensive strategies in secret.**

**While lawmakers look to add to CyberCom’s arsenal, however, the organization is still weighing with the White House how — and under what circumstances — it can use the tools.** Much of the debate revolves around what constitutes a defense, and whether the force can strike back — or strike first — at enemies who want to do the U.S. harm. Pentagon officials and the administration have been working for years on questions about when, if ever, CyberCom can act outside U.S. military networks without seeking the president’s permission.

Senior defense sources tell POLITICO they envision a hardened set of cyber rules someday that would let the military make quick decisions without going to the White House — like those that allow DOD to approve a fighter pilot shooting down a suspicious aircraft that intrudes on sensitive airspace. But those sources concede CyberCom isn’t there yet.

“I think there’s been a three-year debate that’s largely over how to do this, how the military will use cyber techniques,” said Jim Lewis, senior fellow at the Center for Strategic and International Studies in Washington. A presidential directive issued in 2012 does set the outer bounds for what CyberCom can do, **but the details remain murky. The public,** Lewis said, **would benefit from a more “open discussion” of cyber weapons, much like the one the country has had on nuclear weapons.**

Recent events have brought questions about CyberCom’s role into finer focus. As denial-of-service attacks incapacitated the websites of top U.S. banks earlier this year, Alexander pushed — but failed to win support — for a plan to take out the hackers’ servers, The Washington Post reported. And the 2010 Stuxnet computer worm that targeted an Iranian nuclear facility — a worm developed by the U.S. and Israel, according to The New York Times — has raised broader questions about the U.S. government’s use of cyberweapons.

During his tenure, Alexander has been a frequent presence on Capitol Hill, lobbying for legislation to aid CyberCom’s work. He’s asked Congress, for example, to protect companies from lawsuits in the event they act on government information to fight hackers, POLITICO first reported. The idea, however, has raised red flags among civil liberties groups that don’t want to immunize businesses from litigation if they fail to properly shield consumer data from attacks.

Meanwhile, CyberCom continues to struggle with a more basic challenge — how to meet its own staffing targets.

Alexander, testifying before Congress earlier this year, announced a major reorganization that divided the Pentagon’s cybersecurity units into three distinct forces focused on defending DOD networks, assisting commanders and responding to specific threats. The general’s plan envisioned more than a hundred principal and support teams, bolstered by thousands of cyber warriors.

Finding and training those troops, though, has not been easy. “We are on the right track but are not where we projected to be at this point; we knew we set an aggressive schedule,” said Maj. Gen. Williams. CyberCom is “currently at 50-60 percent of our goals for 2013 and will continue to close the gap in the coming year,” he said.

“Outliers like the sequestration, furloughs and overall budget pressure make this force build even more difficult,” Williams said. “We had to shut down our training programs for this summer and fall, impacting us significantly.”

Now the organization is looking at a future without Alexander. Initially, his departure plans prompted the Obama administration to look at whether to split the military’s cyber arm from the NSA, and the president’s task force on surveillance reform recommended a divorce. But the White House announced it intended to preserve the existing relationship, arguing it’s proven effective at addressing cyber threats.

**Congress, however, remains torn on the issue**. An early draft of the defense authorization bill included plans to study a division of NSA and CyberCom, but that provision was later dropped. Some lawmakers have said they don’t want to make changes that would hamstring CyberCom’s work. Still, other **members of Congress are pushing for civilian leadership at the NSA as part of a broader surveillance reform — a change would likely result in a separation from the Pentagon-led cyber force.**

In many ways, the command is still finding its place in the massive military bureaucracy. As part of the defense bill, Congress authorized a new “interdepartmental team” led by the defense secretary’s office to reorient the military on offensive cyber operations, and it directed the Pentagon to create a “deterrence policy” for cyber adversaries.

So far, lawmakers haven’t touched a bigger debate: whether CyberCom should become its own unified command, like Special Operations Command. Lawmakers for now only want to study such a move as they keep closer watch over the organization’s growth.

“This was a realm that literally didn’t exist a generation ago,” explained Peter Singer, director of the Center for 21st Century Security and Intelligence at The Brookings Institution. “By any kind of measure, cyberspace has become a crucial battleground … [and] the spending, of course, has skyrocketed.”

**This unrestricted pre-emption is a direct result of congressional abdication of war powers – Stuxnet opened the floodgate, and PPD 20 prooves that the Presidents capabilities are being expanded without restraint.**

Walker 8/2/13 (Richard, Pen Name for New York News Producer, American free Press, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME <http://americanfreepress.net/?p=11966#sthash.GqeI03l8.dpuf>)

The very moment United States President Barack Obama authorized the “dropping” of an electronic bomb on Iran’s nuclear industry he crossed a line into a new kind of warfare that could have global consequences today and far into the future. The weapon used against Iran was built with the cooperation of Israel and was named Stuxnet. It was a “worm” that infected the computers running Iran’s nuclear industry. German systems control expert, Ralph Langer, who told the world about Stuxnet, remarked Stuxnet represented a dangerous capability and that its code could be used by hackers and others. In other words, Obama had unleashed a weapon that could be re-engineered by anyone to attack computer networks controlling American infrastructure.

Perhaps the most significant aspect of the Stuxnet attack was it demonstrated how Obama had given to himself new powers to launch a cyberwar against any country without Congressional approval. Unlike conventional war in which soldiers are sent to the front and bombs are dropped from the skies, cyberweapons silently and stealthily attack information systems, as well as financial and power centers. We do not know how many times Obama has used his new Cyber Command unit to attack nations other than Iran.

Obama’s Presidential Policy Directive 20, known as PPD 20, which he signed in October 2012, was a stark example of a power grab to accord to him special powers to launch a cyber war at a moment of his choosing. The Guardian newspaper, which first revealed the existence of the directive, claimed it sought a larger target list for cyber attacks and contemplated the use of cyber weapons within the U.S. if the president gave the green light and only in an emergency. But what kind of emergency remains unclear, as does the list of nations he might target in the future.

**Cyber realism has failed us -- cyber phobia is creating an international arms race**

**Deibert 13** -- Ronald J. Deibert is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests include global security, human rights and the geopolitics of cyberspace and information controls. He has published numerous articles, chapters and books on issues related to technology, media and world politics, including co-authoring the *Tracking Ghostnet* report, which documents an alleged cyberespionage network affecting over 1,200 computers in more than 103 countries. Ronald is co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor, and he presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research* and *Astropolitics*. He is a consultant and adviser to governments, international organizations and civil society/non-governmental organizations on issues relating to cyber security, cybercrime, online free expression and access to information. He is a recipient of the Order of Ontario and Queen Elizabeth II Diamond Jubilee medal, and has a Ph.D. in political science from the University of British Columbia (Ronald J. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace," Internet Government Papers, Paper No. 6, October 2013)

At Georgetown University’s April 2013 conference, International Engagement on Cyber, Eugene Kaspersky, CEO of Kaspersky Labs, delivered a keynote address about the prospects of a coming cyber disaster. His message was alarmist, meant to shock the gathered audience, but he also laid out a silver lining of sorts. After describing all of the enabling conditions that are leading us gradually, but invariably, toward catastrophe (and frankly admitting that even he really had no answers for these problems), he concluded on a cheery note: “we’ll just get through it.” If only it were so easy. The previous evening, another set of keynote addresses was delivered with a complementary theme, this time by Republican State Representative Mike Rogers and the CEO of the cyber-security company Mandiant, Kevin Mandia. Rogers berated the Chinese government for their audacious acts of cyber theft, warned of the growing risks to critical infrastructure and then delivered his coup de grace: the United States needs to stop pussyfooting around, it’s time to take the gloves off; now it’s “game on.” For his part, Mandia talked about his company’s widely publicized and discussed report, which presents evidence that the Chinese Peoples’ Liberation Army was responsible for one of the most notorious China-based hacker groups, APT1.2

Mandia freely admitted the report was coordinated with United States political leadership (including military, law enforcement and intelligence). The government had been briefed and, Mandia implied, even had a hand in the timing of the release. Said Mandia, “we’re all ex-military, ex-intel guys” — suggesting comfortably close collaboration between his company and the government. **For that reason, China and the rest of the world saw the report as a strategic escalation, a ratcheting up of the heated rhetoric between the United States and China around cyber-security** issues

Rogers and Mandia are examples of a new, powerful logic emanating from inside “the Beltway,” but rippling across the planet. Government and private sector officials are working increasingly in tandem, united around a realpolitik approach to the challenges of cyber security, buttressed by a burgeoning security industrial complex reaping the economic windfall of the cyber-security market in an era of otherwise economic austerity.

The keynotes were also illustrative of something else: a sombre outlook on all things cyber. The Internet began with great hopes and expectations of liberation. Today, unfortunately, **we live in a time of increasing cyber phobia**. Cyber espionage and warfare, the growing menaces of cybercrime and data breaches, and the rise of new social movements such as WikiLeaks and Anonymous have vaulted cyber security to the top of the international political agenda.4 Almost every day a new headline screams about a serious problem in cyberspace that demands immediate attention. **There is a palpable urgency to act, defend against threats and build up capabilities to deter. But as ominous as the dark side of cyberspace may be, our collective reaction may become the darkest driving force of all.** Where all this will lead is anyone’s guess, but **the constellation of factors contributing to a kind of perfect storm in cyberspace are strong and growing.**

This paper is divided into two parts, each reflecting a different meaning of a concept developed in Daniel Deudney’s (1997) book *Bounding Power*. The first half focusses on the forces that are contributing to escalating international tensions and conflicts in cyberspace, largely driven by state-based concerns around national security. From this perspective, the exercise of state power in cyberspace is growing (to borrow an old phrase) in “leaps and bounds.” The second half employs a different meaning of “bounding power,” that which refers to tying down, checking or restraining the exercise of power, and outlines steps that might be taken to lead us down an alternative path, whereby security and openness are both protected and preserved. There is far more attention paid to conflict than to cooperation in cyber-security matters these days. Lessons of cooperation in other areas of international security that might be applied to the cyber domain are drawn upon in this section. Together, these steps are seen as a kind of “arms control” in cyberspace, in a very broad sense of the term. Arms control in cyberspace has been dismissed as irrelevant at best, or a political ruse at worst. There is not only merit in the concept, but at its heart is the recipe for a comprehensive approach to cyber security that secures a well-functioning global communications system without undermining political liberties. The principal argument is that the instinctive tendency to turn to realpolitik around cyber security is ultimately self-defeating, and that liberal democratic countries should pay more attention to bounding power in cyberspace, domestically and internationally, for both political and technical reasons.

#### Specifically, Our pre-emption policy has created a cyber cold-war

Benavides 7/30/13 (Stephen Benavides is a policy analyst and union organizer from Dallas. He holds a bachelor's degree in political science from the University of North Texas and has done graduate research in econometrics and economic theory. , “The Coming Cyber-Cold War: US Pioneering Online Attacks”, <http://truth-out.org/news/item/17714-the-coming-cyber-cold-war>)

The US government is openly and actively engaged in a reincarnation of the Cold War. Physical assets such as spies and informants have been replaced with zero-day software exploits and network security analysts. Old-school intelligence gathering, while effective to some degree, pales in comparison with the scope of big-data firms such as Endgame and Palantir. Instead of war-ravaged proximity states in Eastern Europe or the Middle East, we have shadowy "actors in cyberspace" and network backdoors on the Internet. The development and expansion of cyber-security, and hence cyber-warfare - equivalent to an arms race - has been in the works for decades and is now a prime objective for the executive branch and the Department of Defense. As the US prepares to deploy weaponized malware and viruses against its enemies, it is forcing those enemies to respond in kind. We are witnessing the first stage of an America-led arms race that undoubtedly will result in a cyber cold war.

Before Edward Snowden released details about foreign and domestic spying program PRISM, low-level and continuous cyber espionage was well underway. As far back as 2002, a three-year attack accessed and downloaded 10 to 20 terabytes of sensitive information from the Department of Defense in an operation titled "Titan Rain." The culprit - whether an individual or a state - was never identified. In 2009, there were cyber attacks on the US water and sewage systems, as well as the national electrical grid. China and Russia are alleged to have accessed secure systems and mapped out the entire infrastructure of the country. More recently, the Obama administration was forced to admit that it had deployed Stuxnet against Iranian nuclear centrifuges and that the NSA attacked Tsinghua University, a research facility in China.

"Cyber warfare attacks" are the new terrorism, with risk to economic and national security elevated to Orwellian heights found post-9/11. At least that's what US military commanders want the public to believe.

#### Un-regulated offensive postures uniquely are bad – Complexity and inter-connected infrastructures means any pre-emption is BOUND to escalate

Benavides 7/30/13 (Stephen Benavides is a policy analyst and union organizer from Dallas. He holds a bachelor's degree in political science from the University of North Texas and has done graduate research in econometrics and economic theory. , “The Coming Cyber-Cold War: US Pioneering Online Attacks”, <http://truth-out.org/news/item/17714-the-coming-cyber-cold-war>)

The unregulated nature of the cyber arms trade not only leaves open the possibility of technology falling into an opposition organization's possession, but guarantees it. Once again, the US is leading weapons proliferation. Political inconvenience of a militarized conventional war also may play a part in the burgeoning cyber war. It is much more difficult for military commanders to justify the death of a sister or brother in combat operations widely understood to be about maintaining access to energy resources than a "victimless" attack on a foreign government to protect internal bank documents or dam vulnerabilities.

The government does acknowledge that the directive may raise unique national security and foreign policy concerns, and it states, "DCEO (Defensive Cyber Effects Operations) and OCEO (Offensive Cyber Effects Operations), even for subtle or clandestine operations, may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect U.S. national interests in many locations." One issue with waging war in an unknown environment, often against unknown enemies, is that an actor is unable to predict with any accuracy how weaponized software may interact with different systems. Even the most professional attacks have been known to spiral out of control, which leaves open the risk that an attack on an enemy ultimately will affect those it was designed to "protect."

Governments have not moved to apply international laws of war to cyberspace, although they call it warfare nonetheless. The Pentagon says the same rules of engagement apply, which is patently false because the US is under constant attack and also is attacking every day. Where is the open declaration of war? There is none. Instead the Internet is a militarized proxy, a theater for a new cold war. And anyone who wants to participate can. It took only 20 years for the parent of the Internet, the US military, to exercise overwhelming influence on its once-free and forlorn child. The Internet is now, or maybe has always been, an agent of the state.

#### Lack of civilian bureaucratic control make conflict inevitable

Austin 8/6/13 (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.

In 1969, the USSR acted first to propose an end to the race for the technological frontier of nuclear weapons because it knew it was losing the contest and because it knew there was political sentiment in the United States and in its Allied countries that supported limitations on the unbridled nuclear fetish.

As we ponder the American cyber industrial complex of today, we see a similar constellation of opposition to its power emerging. This constellation includes not just the political rivals who see they are losing in cyber space (China and Russia), but nervous allies who see themselves as the likely biggest victims of the American race for cyber superiority, and loyal American military commanders who can see the risks and dangers of that quest.

It is time for the United States to take stock of the collateral damage that its quest for cyber military power, including its understandable quest for intelligence superiority over the terrorist enemy, has caused amongst its allies. The loss has not yet been seen at the high political level among allies, in spite of several pro forma requests for information from countries such as Germany. The loss of U.S. credibility has happened more at the popular level. Around the world, once loyal supporters of the United States in its war on terrorism had a reasonable expectation to be treated as faithful allies. They had the expectation, perhaps naïve, that privacy was a value the Americans shared with them. They did not expect to be subject to such a crude distinction (“you are all non-Americans now”). They did not want to know that their entire personal lives in cyber space are now recoverable – should someone so decide – by the running of a bit of software in the NSA. After the Prism revelations, so many of these foreign citizens with an internationalist persuasion and solidarity for the United States now feel a little betrayed.

Yet, in the long run, the most influential voice to end the American quest for cyber military superiority may come from its own armed forces. There are military figures in the United States who have had responsibility for nuclear weapons command and control systems and who, in private, counsel caution. They advocate the need to abandon the quest for cyber dominance and pursue a strategy of “mutual security” in cyber space – though that has yet to be defined. They cite military exercises where the Blue team gets little or no warning of Red team disruptive cyber attack on systems that might affect critical nuclear command and control or wider war mobilization functions. Strategic nuclear stability may be at risk because of uncertainty about innovations in cyber attack capability. This question is worth much more attention.

U.S. national security strategy in cyber space needs to be brought under stronger civilian oversight and subject to more rigorous public scrutiny. The focus on Chinese cyber espionage has totally preempted proper debate about American cyber military power. Most in the United States Congress have lined up to condemn Snowden. That is understandable. But where are the critical voices looking at the bigger picture of strategic instability in cyberspace that existed before Snowden and has now been aggravated because of him? The Russian and Chinese rejections of reasonable U.S. demands for Snowden’s extradition may be every bit as reasonable given their anxiety about unconstrained American cyber superiority.

#### US cyber attacks inevitably escalate to kinetic war

Moss 4/19/13 (Trefor, covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009 The Diplomat- - “Is Cyber War the New Cold War?”, <http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/3/>)

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.

But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare’s new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?

For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations – repeated attacks followed by often flimsy denials – almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.

The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China – Google and The New York Times being just two of the most high-profile victims – and which President Obama has now insisted are at least partly state-sponsored.

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations.

As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21st century reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Uniquely true because of mis-perceptions

Rosenzweig 9, Professor at Georgetown Law

(Paul, founder of Reid Branch Consulting, specializing in homeland security, senior advisor to the Chertoff Group, Carnegie Fellow at Northwestern, professor at National Defense University, Editorial board at the Journal of National Security Law & Policy, deputy assistant secretary for policy at the US Department of Homeland Security, "National Security Threatsin Cyberspace" merican Bar Association Standing Committee on Law and National Security And National Strategy Forum, September 2009, [www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf](http://www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf))

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122 Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

#### This is particularly true of bureaucratic decision makers and cyber war who have a “do something” mentality

Owens et al. 09 (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, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, pdf)

If an adversary conducts a cyberattack against the United States, a first question for U.S. decision makers will be knowledge of the attack’s impact and magnitude. Such knowledge is necessary to inform an appropriate U.S. response. (If, for example, the United States wishes to make a commensurate response, it needs to know what parameters of the incoming attack would characterize a commensurate response.)

But in many kinds of cyberattack, the magnitude of the impact of the first cyberattack will be uncertain at first, and may remain so for a considerable period of time. Decision makers may then be caught between two challenges—a policy need to respond quickly and the technical fact that it may be necessary to wait until more information about impact and damage can be obtained. (As noted in Section 2.5, these tensions are especially challenging in the context of active defense.)

Decision makers often feel intense pressure to “do something” immediately after the onset of a crisis, and sometimes such pressure is warranted by the facts and circumstances of the situation. On the other hand, the lack of immediate information may prompt decision makers to take a worst-case view of the attack and thus to assume that the worst that might have happened was indeed what actually happened. Such a situation has obvious potential for inappropriate and unintended escalation.

#### Status quo lack of congressional checks on offensive cyber operations violates legal norms of conflict --- restrictions are key

Dycus 10 (Professor Stephen Dycus is an internationally recognized authority on national security law and environmental law. The courses he has taught at Vermont Law School include Public International Law, National Security Law, Estates, Property, and Water Law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. (Stephen, "Congress' Role in Cyber Warfare," National Security Journal, Volume 4, Issue 155, 2010 <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

#### Only congress establishing a framework solves executive overreach.

HOLMES 08 Walter E. Meyer Professor of Law at NYU School of Law [Stephen Holmes, “Conclusion,” from Security v. Liberty: Conflicts Between Civil Liberties and National Security in American History, ed by Daniel Farber] page 218-219

A refusal to listen to criticism is dismaying precisely because the threat we face is so new and elusive and the resources we have at our disposal (soldiers, Arabic speakers, satellite coverage, the attention span of high officials, and so on) remain scarce. The extreme difficulty of setting priorities among low-probability catastrophic threats in the war on terror strongly suggests the need to **revitalize various mechanisms of political self-correction**, including after-action reviews and mandatory second opinions. Consultations with knowledgeable parties outside a narrow circle of like-minded operatives committed to upholding a party line should be not optional but obligatory. Because the country had never before faced a threat anything like that posed by private sector nuclear terrorism, the administration's first responses were destined to be experimental and plagued by mistakes. To respond intelligently, therefore, it should have safeguarded and fortified all existing decision-making protocols containing even residual elements of adversarial process.

Because the war on terror is totally unprecedented, giving unsupervised discretion to a single clique inside one compartment of the executive without requiring obligatory consultations with knowledgeable parties cannot possibly be prudent. The aim of liberal institutions should be to facilitate the psychologically painful process of recognizing past blunders and initiating requisite midstream readjustments. Preserving public liberty means frustrating the impulse of incumbents to silence their critics. The payoff, on balance, is more thoughtful policy. The worst imaginable decision making system for managing an unprecedented threat that is frustratingly difficult to assess is unchecked presidential discretion, because chief executives are bound to be inhibited by authorial pride from expeditiously correcting their most damaging missteps.

Not only do powerful men dislike admitting their mistakes. Multiparty democracy joins perverse institutional incentives to those stemming from ordinary human vanity. Competitive elections make incumbents view admission of error in questions of national security as a gift to their partisan rivals. Such a problem is so serious, in fact, that it might lead us to invert the conservative mantra that liberal constitutionalism is a suicide pact. Observing the disaster of the Iraq war, we can conclude that granting unfettered discretion to the commander in chief is the real suicide pact. Freeing a poorly equipped individual from all constitutional checks and balances and allowing a president to engage the American military in bloody foreign adventures without giving plausible reasons for his action is a perfect formula for creating the debacle facing us today.

important to a nation), a regulatory regime for cyberattack might also reduce the likelihood of economic warfare using this military tool.

**Congressional opposition to the authority curbs Presidential action – robust statistical and empirical proof**

KRINER 10 Assistant professor of political science at Boston University [Douglas L. Kriner, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, page 228-231]

Conclusion

The sequence of events leading up to the sudden reversal of administration policy and the dramatic withdrawal of U.S. Marines from Lebanon clearly demonstrates that open congressional opposition to Reagan's conduct of the mission in Beirut was critically important in precipitating the change in course. By tracing the pathways of congressional in- fluence, the case study achieves two important objectives. First, it vividly illustrates Congress's capacity to influence the scope and duration of a use of force independent of major shifts in public opinion and changing conditions on the ground. The analysis makes clear that there was no dramatic shift in public opinion after the Beirut barracks bombing that compelled the Reagan administration to withdraw the Marines; in fact, in the wake of the attack the public rallied behind the president. As such, opponents of Reagan's policies in Congress initially fought against the tide of public opinion, and the modest decline in popular support for the president's handling of the Lebanon mission occurred only after a sustained campaign against the deployment on Capitol Hilt.89 Similarly, the administration's own internal analysis of the situation in early January 1984 makes clear that changing conditions on the ground did not necessitate a dramatic change in the nature of the Marine mission. Indeed, by the National Security Council's own estimate, some conditions in the region were actually improving. Instead, administration officials repeatedly emphasized domestic pressures to curtail the scope and duration of the Marine mission.90 Moreover, as the political and military situation in Lebanon worsened in late January and early February 1984, it is interesting that a number of key administration officials publicly and privately believed that there was a direct link between congressional opposition at home and the deterioration of the situation on the ground in the Middle East.

Second, the case study illustrates how the formal and informal congressional actions examined in the statistical analyses of chapter 4 affected presidential decision-making through the proposed theoretical mechanisms for congressional influence over presidential conduct of military affairs developed in chapter 2. Vocal opposition to the president in Congress-expressed through hearings and legislative initiatives to curtail presidential authority, and the visible defection from the White House of a number of prominent Republicans and erstwhile Democratic allies-raised the political stakes of staying the course in Lebanon. Nothing shook Reagan's basic belief in the benefits to be gained from a strong, defiant stand in Beirut. But the political pressure generated by congressional opposition to his policies on both sides of the aisle raised the likely political costs of obtaining these policy benefits. Congressional opposition also influenced the Reagan administration's decision-making indirectly by affecting its estimate of the military costs that would have to be paid to achieve American objectives. In the final analysis, through both the domestic political costs and signaling mechanisms discussed in chapter 2 , congressional opposition contributed to the administration's ultimate judgment that the benefits the United States might reap by continuing the Marine mission no longer outweighed the heightened political and military costs necessary to obtain them.

Finally, while the Marine mission in Lebanon is admittedly but one case, it is a case that many in the Reagan administration believed had important implications for subsequent military policymaking. In a postmortem review, Don Fortier of the National Security Council and Steve Sestanovich at the State Department warned that the debacle in Lebanon raised the possibility that, in the future, the decision to use force might be akin to an all-or-nothing decision. "If the public and Congress reject any prolonged U.S. role (even when the number of troops is small)," the administration analysts lamented, "we will always be under pressure to resolve problems through briefer, but more massive involvements-or to do nothing at all." Thus, from the administration's "conspicuously losing to the Congress" over Lebanon policy, Fortier and Sestanovich argued that the White House would have to anticipate costly congressional opposition if similar actions were launched in the future and adjust its conduct of military operations accordingly, with the end result being a "narrowing of options" on the table and more "limited flexibility" when deploying major contingents of American military might abroad.91 This last point echoes the first anticipatory mechanism posited in chapter 2, and reminds us that Congress need not overtly act to rein in a military action of which it disapproves for it to have an important influence on the scope and duration of a major military endeavor. Rather, presidents, having observed Congress's capacity to raise the political and tangible costs of a given course of military action, may anticipate the likelihood of congressional opposition and adjust their conduct of military operations accordingly.

**Our discussion of cyber policy is critical – only that can spill over to grassroots movements that prevent reckless use of OCOs**

**Deibert 13** -- Ronald J. Deibert is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests include global security, human rights and the geopolitics of cyberspace and information controls. He has published numerous articles, chapters and books on issues related to technology, media and world politics, including co-authoring the *Tracking Ghostnet* report, which documents an alleged cyberespionage network affecting over 1,200 computers in more than 103 countries. Ronald is co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor, and he presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research* and *Astropolitics*. He is a consultant and adviser to governments, international organizations and civil society/non-governmental organizations on issues relating to cyber security, cybercrime, online free expression and access to information. He is a recipient of the Order of Ontario and Queen Elizabeth II Diamond Jubilee medal, and has a Ph.D. in political science from the University of British Columbia (Ronald J. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace," Internet Government Papers, Paper No. 6, October 2013)

What is remarkable is that the Internet functions precisely because of the absence of centralized control, because of the thousands of distributed, loosely coordinated monitoring mechanisms.32 While these decentralized mechanisms are not perfect and can occasionally fail, they can also form the basis of a coherent distributed security strategy. Bottomup, grassroots solutions to the Internet’s security problems are consistent with principles of openness, avoid heavy-handedness and provide checks and balances against the concentration of power. Part of a distributed security strategy should enable ways to facilitate cooperation among the existing, largely scattered security networks while making their actions more transparent and accountable. These technical steering functions should be preserved as much as possible along the lines of reputationbased and independently distributed governance mechanisms in order to support an open yet secure communications space.

In other words, rather than abolish this system for another, more top-down approach, it should be buttressed and amplified. Loosely structured but deeply entrenched networks of engineers, working on the basis of credible knowledge and reputation, whose mission and *raison* d’être is to focus on cyberspace itself and its secure functioning to the exclusion of all else, are essential to its sustenance and security. We need to build out and give room and space for those networks to thrive internationally, rather than co-opt their talents for national security projects that create international divisions and rivalry.

One factor that would help facilitate such a development would be to conscientiously avoid the rhetoric of warfare and weapons in descriptions of threats and issues that are largely criminal in nature. Far too often, military and intelligence agencies are given deference in responses to areas from which they should more properly be excluded altogether. Lessons from the nuclear era could be drawn here as well. University of Toronto international relations theorist Emanuel Adler undertook a seminal study of the learning among Russian and US nuclear scientists during the Cold War, leading to the eventual development of a transnational epistemic community around nuclear arms control.33 Critical to the success of this process was the engagement of scientists, engineers and civilian bodies with each other, unencumbered by the national defence agencies operating at higher levels. While Reaganera mythology attributes the end of the Cold War to the United States outspending the Soviet Union, arguably just as important was the learning and trust among this epistemic community that contributed to the war’s end. A page could be taken from this process and applied to supporting transnational networks of civilian engineers, scientists and practitioners in the cyber domain.

Arms control is almost always thought of as a set of practices that apply to states. But in light of the fact that the vast majority of cyberspace is owned privately, the same basic premise of oversight and accountability must also extend to the private sector. Civic networks like those that helped spawn the Arab Spring are inherently transnational and have a vital role to play in monitoring the globe-spanning corporations that own and operate cyberspace. Persistent public pressure, backed up by credible evidence-based research and campaigns (such as the Electronic Frontier Foundation’s privacy scorecard), are the best means to ensure the private sector complies with human rights standards worldwide. Civic networks must also make the case that government pressures to police the Internet impose costly burdens on businesses that should be conceded only with the greatest reservations and proper oversight. Efforts to promote greater corporate social responsibility in the cyber domain, such as the Global Network Initiative, fit **squarely into the distributed security model and should be encouraged**. When complemented by government regulations that set standards around breach disclosures and respect for human rights abroad, a robust set of checks and balances can be developed, at least in the liberal democratic core, before gradually moving outward. One area where such restraints should be explored is around the growing cyber-security market, particularly those technologies that clearly have offensive uses. The European Parliament has been debating end-use based restrictions on this trade

Others think that’s futile.36 The US Department of State has issued guidance on the export of “sensitive technologies” to Iran and Syria pursuant to the applicable sanctions regimes.37 Human rights organizations have filed complaints against Gamma International,38 and Citizen Lab urged investor activism39 when it discovered that Blue Coat Systems was owned, in part, by the Ontario Teachers’ Pension Plan. To be sure, there are no easy or simple answers to this market and it’s not clear that more government regulations or laws are the answer. **But it is clear that greater vigilance and oversight are necessary,** and that we cannot rely on market forces and corporate social responsibility to take care of negative uses on their own.

Universities have a special role to play as stewards of an open but secure cyberspace, since it was from “the university” that the Internet was born, and from which its guiding principles of peer review and transparency were founded. Protected by academic freedom, equipped with advanced research resources that span the social and natural sciences, and distributed across the world, university-based research networks are essential custodians and monitors of an open and secure cyberspace.

Finally, bounding power in cyberspace will require a general attitude shift among users as to how they approach cyberspace. There is a paradox today: as never before we are surrounded by technology, and yet as never before do we, the users, know so little about how that technology functions. For most of us, it is indeed the “consensual hallucination” that novelist William Gibson once defined — always on, always working, 24/7, like running water. It is this obliviousness to what goes on beneath the surface that allows such untrammelled violations of privacy to occur. Shifting this attitude will not be easy. Cyberspace is an extraordinarily complex technological environment, and it gets more complex with each passing day. Furthermore, there are considerable disincentives to having average people “lifting the lid” on the technology, including secrecy laws and intellectual property protections. **However, an essential check on the abuse of power in cyberspace must come from changing this social outlook from the ground up. Citizens must be encouraged to not accept the technological infrastructure of cyberspace and its services for granted. Lifting the lid on the Internet should be encouraged as a kind of civic virtue.**

**Appeals for institutional restrain are a crucial supplement to political resistance to executive power.**

David **COLE** Law @ Georgetown **’12** “The Politics of the Rule of Law: The Role of Civil Society in the Surprising Resilience of Human Rights in the Decade after 9/11” http://www.law.uchicago.edu/files/files/Cole%201.12.12.pdf p. 51-53

As I have shown above, while political forces played a significant role in checking President Bush, what was significant was the particular substantive content of that politics; it was not just any political pressure, but pressure to maintain fidelity to the **rule of law**. Politics standing alone is as likely to fuel as to deter executive abuse; consider the lynch mob, the Nazi Party in Germany, or xenophobia more generally. What we need if we are to check abuses of executive power is a politics that **champions the rule of law**. Unlike the politics Posner and Vermeule imagine, this type of politics cannot be segregated neatly from the law. On the contrary, it **will often coalesce around a distinctly legal challenge,** objecting to departures from **distinctly legal norms**, heard in a court case, as we saw with Guantanamo. Congress’s actions make clear that had Guantanamo been left to the political process, there would have been few if any advances. The litigation generated and **concentrated** **political pressure** on claims for a **restoration** of the values of **legality**, and, as discussed above, that pressure then played a critical role in the litigation’s outcome, which in turn affected the political pressure for reform. There is, to be sure, something paradoxical about this assessment. The rule of law, the separation of powers, and human rights are designed to discipline and constrain politics, out of a concern that pure majoritarian politics, focused on the short term, is likely to discount the long-term values of these principles. Yet without a critical mass of political support for these legal principles, they are unlikely to be effective checks on abuse, for many of the reasons Posner andVermeule identify. The answer, however, **is not to abandon the rule of law for politics, but to develop and nurture a political culture that values the rule of law itself.** Civil society organizations devoted to such values, such as Human Rights Watch, the Center for Constitutional Rights, and the American Civil Liberties Union, play a central role in facilitating, informing, and generating that politics. Indeed, they have no alternative. Unlike governmental institutions, civil society groups have no formal authority to impose the limits of law themselves. Their recourse to the law’s limits is necessarily indirect: they can file lawsuits seeking judicial enforcement, lobby Congress for statutory reform or other legislative responses, or seek to influence the executive branch. But they necessarily and simultaneously pursue these goals through political avenues – by appealing to the public for support, educating the public, exposing abuses, and engaging in public advocacy around rule-of-law values. Unlike ordinary politics, which tends to focus on the preferences of the moment, the politics of the rule of law is committed to a set of long-term principles. Civil society organizations are uniquely situated to bring these long-term interests to bear on the public debate. Much like a constitution itself, civil society groups are institutionally designed to emphasize and reinforce our long-term interests. When the ordinary political process is consumed by the heat of a crisis, organizations like the ACLU, Human Rights First, and the Center for Constitutional Rights, designed to protect the rule of law, are therefore especially important. While Congress and the courts were at best compromised and at worst complicit in the abuses of the post-9/11 period, civil society performed admirably. The Center for Constitutional Rights brought the first lawsuit seeking habeas review at Guantanamo, and went on to coordinate a nationwide network of volunteer attorneys who represented Guantanamo habeas petitioners. The ACLU filed important lawsuits challenging secrecy and government excesses, and succeeded in disclosing many details about the government’s illegal interrogation program. Both the ACLU and CCR filed lawsuits and engaged in public advocacy on behalf of torture and rendition victims, and challenging warrantless wiretapping. Human Rights Watch and Human Rights First wrote important reports on detention, torture, and Guantanamo, and Human Rights First organized former military generals and admirals to speak out in defense of humanitarian law and human rights. These efforts are but a small subset of the broader activities of civil society, at home and abroad, that helped to bring to public attention the Bush administration’s most questionable initiatives, and to portray the initiatives as contrary to the rule of law. At their best, civil society organizations help forge a politics of the rule of law, in which there is a **symbiotic relationship** between politics and law: the appeal to law informs a particular politics, and that politics reinforces the law’s appeal, in a mutually reinforcing relation. Posner and Vermeule understand the importance of politics as a checking force in the modern world, but fail to see the critical qualification that the politics must be organized around a commitment to fundamental principles of liberty, equality, due process, and the separation of powers – in short, the rule of law. Margulies and Metcalf recognize that politics as much as law determines the reality of rights protections, but fail to identify the unique role that civil society organizations play in that process. It is not that the “rule of politics” has replaced the “rule of law,” but that, properly understood, a politics of law is a critical supplement to the rule of law. We cannot survive as a constitutional democracy true to our principles without both. And our survival turns, not only on a vibrant constitution, but on a vibrant civil society dedicated to reinforcing and defending constitutional values.

**Our discussion raises awareness of cyber militarism and spills over to policy**

**Owens et al. 09** (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, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, pdf)

A historical analogy might be drawn to the study of nuclear issues. In many ways, today’s state of affairs regarding public discourseon cyberattack is analogous to the nuclear debate of 50 years ago. At that time, nuclear **policy issues were veiled in** secrecy, and there was **little public debate** about them. Herman Kahn’s books (On Thermonuclear War, Thinking the Unthinkable) were the first that addressed in the open literature what it might mean to fight a nuclear war. These **seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a real impact on nuclear policy**. From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that **it deserves robust and open discussion and debate**, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some **common foundation of information about the topic at hand.** Thus, **the report’s role in providing education and background is in our view its most important function.**

**Even if our solution isn't perfect, the 1ac is a step in the right direction -- individual acknowledgement of our agency in cyber security discussions is a critical pre-requisite the re-shaping the terrain of cyber policy**

**Deibert 13** -- Ronald J. Deibert is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests include global security, human rights and the geopolitics of cyberspace and information controls. He has published numerous articles, chapters and books on issues related to technology, media and world politics, including co-authoring the *Tracking Ghostnet* report, which documents an alleged cyberespionage network affecting over 1,200 computers in more than 103 countries. Ronald is co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor, and he presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research* and *Astropolitics*. He is a consultant and adviser to governments, international organizations and civil society/non-governmental organizations on issues relating to cyber security, cybercrime, online free expression and access to information. He is a recipient of the Order of Ontario and Queen Elizabeth II Diamond Jubilee medal, and has a Ph.D. in political science from the University of British Columbia (Ronald J. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace," Internet Government Papers, Paper No. 6, October 2013)

Looking toward the near term in cyberspace governance, there are many possible scenarios, with unforeseen contingencies taking us down any number of paths. At the same time**, politics and society are not entirely chaotic**: social order is shaped by underlying forces that set the tempo and framework within which life unfolds. Today, these forces appear to be driving securitization processes in cyberspace, processes that may end up subverting the domain entirely, possibly leading to system wide instability and perhaps even international violence**. It is imperative that we use our agency to check and constrain the least desirable elements of these trends and shape those structures that provide the framework for what is seen as legitimate or** not. Doing so will require a clear vision and a strategy to implement it, which in turn will require coordinated work at multiple levels and involve a wide variety of stakeholders. The obstacles standing in the way of realizing this vision are certainly formidable, but the alternatives to doing nothing are dire. The **securitization of cyberspace may be inevitable, but what form that security takes is not**. As the securing of cyberspace unfolds, ensuring basic principles of transparency, accountability and mutual restraint will be critical.