# UGA 1AC -- Emory KL

### 1AC Plan

#### The United States federal government should require the President of the United States to consult with Congress prior to the use of offensive cyber operations by the United States.

### 1ac -- Preemption

#### Contention 1 is preemption

#### The US is militarizing cyberspace now -- congress still needs to develop guidelines

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 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.

#### 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 proliferation and nuclear war are 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.

#### Kinetic attacks causes nuclear war

Roth 07 professor in IR at Goucher College 7 [Ariel Ilan Roth, “Nuclear Weapons in Neo-Realist Theory”, REFLECTION, EVALUATION, INTEGRATION, International Studies Review, pg 369-384]

Critical, though not explicit, in Waltz is the belief that **a war between nuclear powers will be hard to maintain at the conventional level.** Waltz (Waltz and Sagan 2003:9) allows that such **a sub-nuclear war may be fought but** considers **the risk of it escalating to the nuclear level with its accompanying certain destruction as too high for the risk tolerance of most leaders**. The strategic studies literature has played host to this debate for decades. Some, like Snyder (1965), have argued that **nuclear weapons are**, in a sense, **mutually negating, creating what has been called the stability-instability paradox, wherein stability at the nuclear level breeds instability at the conventional level**. It is, in this conception, as if two duelists stand with guns loaded and cocked at each other’s heads yet proceed to have their fight with daggers instead (Jervis 1989:19-20). Others, like Barry Posen (1982), have argued that **even though nuclear states may wish to limit their conflict to conventional weapons**, actions that occur during wartime can lead to what he calls “inadvertent escalation.” In his “Cold War Turned Hot” example, NATO attacks near Soviet ballistic submarine bases could draw a nuclear response even though the aim of NATO is not to harm the strategically stabilizing Soviet submarine-based missile arsenal (Posen 1982:29-30). Such an interaction would then escalate further as American targets were hit with nuclear weapons and a war that was supposed to be both limited and sub-nuclear is now an apocalyptic doomsday. **The prospects for inadvertent escalation are recognized by Jervis** (1989:21) as well who comments that “**because escalation can occur although no one wants it to, mutual second-strike capability does not make the world safe for major provocations and limited wars**.” This conclusion leads to the first of Jervis’ (1989:23-24) expected outcomes from what he calls the “nuclear revolution,” namely, that there will be peace among the great powers.

#### 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 andNational 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

#### Independently – Cyber attacks breaks down command and control – causes nuclear response. The bureaucratic decision to react without information is a result of situating offensive cyber ops with the president

Cimbala 11(Stephen J. Cimbala 2011. Professor of Political Science at Penn State. “Nuclear Crisis Management and “Cyberwar” Phishing for Trouble?” Strategic Studies Quarterly Spring 2011)

This section discusses how cyberwar might adversely affect nuclear crisis management. Readers are advised, however, that history is indeterminate.It might turn out that, in some fortuitous cases, the United States coulduse nuclear deterrence and cyberwar as joint multipliers toward a success-ful outcome in crisis or war. For example, in facing down an opponentwith a comparatively small or no nuclear arsenal and inferior conventionalstrike capabilities, the United States or another power could employ infor-mation warfare aggressively “up front” while forgoing explicit mention ofits available nuclear capability. Russia’s five-day war against Georgia inAugust 2008 involved obvious cyber attacks as well as land and air opera-tions, but no explicit nuclear threats. On the other hand, had Georgia al-ready been taken into membership by NATO prior to August 2008 or hadRusso-Georgian fighting spread into NATO member-state territory, thevisibility of Russia’s nuclear arsenal as a latent and potentially explicitthreat would have been much greater.Notwithstanding the preceding disclaimers, information warfare has the potential to attack or disrupt successful crisis management on each offour dimensions. First, it can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Sup-pose one side plants a virus or worm in the other’s communications net-works.19 The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make itmore difficult for the cyber victim to arrange a military attack. But de-stroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A mayintend to signal “resolve” instead of “yield” to its opponent on a particularissue. Side B, misperceiving a “yield” message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dan-gerous situation to develop.Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of un-anticipated problems, from the standpoint of civil-military relations, arepossible under these conditions. First, political leaders may have pre-delegated limited authority for nuclear release or launch under restric-tive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized toemploy nuclear weapons distributed within their command. Clogged,destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was.During the Cold War, for example, disrupted communications betweenthe US National Command Authority and ballistic missile submarines,once the latter came under attack, could have resulted in a joint decisionby submarine officers to launch in the absence of contrary instructions.Second, information warfare during a crisis will almost certainly in-crease the time pressure under which political leaders operate. It may dothis literally, or it may affect the perceived timelines within which thepolicymaking process can make its decisions. Once either side sees parts ofits command, control, and communications (C3) system being subvertedby phony information or extraneous cyber noise, its sense of panic at thepossible loss of military options will be enormous. In the case of US ColdWar nuclear war plans, for example, disruption of even portions of thestrategic C3 system could have prevented competent execution of parts ofthe SIOP (the strategic nuclear war plan). The SIOP depended upon finelyorchestrated time-on-target estimates and precise damage expectanciesagainst various classes of targets. Partially misinformed or disinformednetworks and communications centers would have led to redundant at-tacks against the same target sets and, quite possibly, unplanned attacks onfriendly military or civilian installations.A third potentially disruptive effect of infowar on nuclear crisis man-agement is that it may reduce the search for available alternatives to thefew and desperate. Policymakers searching for escapes from crisis denoue-ments need flexible options and creative problem solving. Victims of in-formation warfare may have a diminished ability to solve problems routinely,let alone creatively, once information networks are filled with flotsam andjetsam. Questions to operators will be poorly posed, and responses (ifavailable at all) will be driven toward the least common denominator ofpreviously programmed standard operating procedures. Retaliatory sys-tems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives: A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.20 The propensity to search for the first available alternative that meetsminimum satisfactory conditions of goal attainment is strong enough undernormal conditions in nonmilitary bureaucratic organizations.21 In civil-military command and control systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last; or so policymakers and their military advisors may persuade them-selves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, a number of members of thepresidential advisory group continued to propound an air strike and inva-sion of Cuba during the entire 13 days of crisis deliberation. Had less timebeen available for debate and had President Kennedy not deliberatelystructured the discussion in a way that forced alternatives to the surface,the air strike and invasion might well have been the chosen alternative.22Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side’s intentions and capabilities to be conveyed tothe other, with potentially disastrous results. Another example from theCuban crisis demonstrates the possible side effects of simple misunder-standing and noncommunication on US crisis management. At the mosttense period of the crisis, a U-2 reconnaissance aircraft got off course andstrayed into Soviet airspace. US and Soviet fighters scrambled, and a pos-sible Arctic confrontation of air forces loomed. Khrushchev later toldKennedy that Soviet air defenses might have interpreted the U-2 flight asa prestrike reconnaissance mission or as a bomber, calling for a compensa-tory response by Moscow.23 Fortunately Moscow chose to give the UnitedStates the benefit of the doubt in this instance and to permit US fightersto escort the wayward U-2 back to Alaska. Why this scheduled U-2 mis-sion was not scrubbed once the crisis began has never been fully revealed;the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of “normal” reconnaissance under these extra-ordinary conditions.

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

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.

#### CERTAIN CONGRESSIONAL Consultation is necessary – preemption is inevitable without congressional checks. Decreasing BUREAUCRATIC INERTIA in response to a cyber attack is the only way to avoid conflict.

Dycus 10 (Professor Vermont Law School, “Congress’s Role in Cyber Warfare”, 8/11/2010, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. 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 ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 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. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential 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.

### 1ac -- China

**Contention 2 is China:**

#### This lack of legal codification has blurred the lines between non-destructive and incredibly destructive cyberattacks which lowers the threshold for escalatory cyberwarfare

Loon 12 (Collin Engelbert Peter van Loon Royal Netherlands Army , “Offensive Cyber What are the possibilities of the use of offensive cyber as an offensive capability within the existing international legal framework?”, https://cyberwar.nl/d/MSc-thesis\_Offensive-Cyber\_Collin-van-Loon\_June-2012.pdf)

Offensive cyber operations are not covered by an international agreed legal framework. The consequence is that it is hard to distinguish between the different kind of cyber attacks, their purpose, their origin and under which existing law the attacks fall. LoAC only covers the jus i bello kind of attacks. When the LoAC were first drafted, only nation-states had the legal ability to wage war and to execute operations. Since cyber attack weapons are easy available for everyone, non-state actors and even individuals are capable getting involved in cyber incidents, cyber operations or cyber conflict. Thus, the lines between state, non-state, and individual attackers are unclear in a legal regime that discriminates between LoAC on the one hand and national criminal laws and law enforcement on the other (Dam et al., 2009, s. 22).

The lack of a decent legal framework also endangers a decent distinction between cyber attacks conducted in the cause of warfare, or cyber attacks as a simple hacker’s activity in the cause of law enforcement. The means and methods used by a nation-state to conduct cyber attacks can vary greatly and can also be classified in a number of ways. However, although this variety, these attacks can be similar if not identical to those used by hackers in the context of cyber crimes. Moreover, cyber attacks can occur both in times of peace and war (Palojärvi, 2009). The blurring in these different types of cyber attack makes the need for a general international accepted cyber legal framework even more necessary

#### Specifically, this hampers efforts at mutual drawdown and cyber de-escalation with China

Sanger 9/1/13 (David, A 1982 graduate of Harvard College, Sanger has been writing for the Times for 30 years covering foreign policy, globalization, nuclear proliferation, and the presidency., He has been a member of two teams that won the Pulitzer Prize, and has been awarded numerous honors for national security and foreign policy coverage. “Documents detail U.S. cyber-espionage plans”, <http://www.thehindu.com/news/international/documents-detail-us-cyberespionage-plans/article5083012.ece>)

231 operations planned for 2011 – both small scale and large scale

Newly disclosed budget documents for America’s intelligence agencies show how aggressively the United States is conducting offensive cyber-operations against other states, even while the Obama administration protests attacks on U.S. computer networks by China, Iran and Russia.

The documents, obtained by The Washington Post from Edward J. Snowden, the former National Security Agency contractor, indicate 231 such operations in 2011, a year after the first evidence emerged of a U.S.-and Israeli-led cyberattack against Iran’s nuclear-enrichment centre.

It suggests that President Barack Obama was not deterred by the disclosure of the Iranian operation, which became evident because of a technological error, and is pressing ahead on using cyber-weapons against a variety of targets.

The Post had said it has withheld most of the 178 pages of documents at the request of government officials because of the sensitivities of the spying operations they describe.

Unlike drone attacks, which the administration has begun to acknowledge publicly and provide legal justifications for, cyberattacks are still regarded as part of a secret arsenal.

The attacks described in the budget documents appear to be on a far smaller scale than the series of attacks on Iran, which were part of a classified operation called “Olympic Games”.

The Post talked of a parallel effort, code-named GENIE, which it described as an effort by U.S. intelligence officials working for the NSA and the military’s Cyber Command to insert surreptitious controls into foreign computer networks. That computer code, a form of malware, allows U.S. officials to hijack the computers or route some of their data to servers that enable U.S. espionage.

It is unclear how many, if any, of those 231 operations are merely for espionage or data manipulation, and how many may be intended to destroy or disable infrastructure. Mr. Obama, in an executive order signed last year, has reserved the right to decide when the United States should conduct such operations. It is not clear how many of the 231 he approved.

Diplomatically, the disclosure of the latest Snowden documents poses a new challenge to Mr. Obama. He has pressed China to cease its own cyber-operations in the United States, many of which are aimed at the theft of intellectual property — including corporate secrets and plans for the F-35 Joint Strike Fighter, the country’s most expensive new weapons system.

The Chinese have responded that America also conducts extensive cyber-operations — including against China — and will doubtless use the most recent disclosures to press that case. So far, Mr. Obama’s effort to get the Chinese engaged in a deeper dialogue on cyberissues has yielded discussions, but little fruit.

#### Lack of legal codification uniquely makes miscalculation likely --- it is a unique escalation scenario for war

VornDick 6/30/13 (Wilson VornDick is a lieutenant commander in the U.S. Navy, where he is assigned to the Pentagon. Previously, he worked at the Chinese Maritime Studies Institute at the U.S. Naval War College. , “The Real U.S.-Chinese Cyber Problem”, <http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796?page=2>)

Recent waves of cyber attacks emanated from China despite their vehement denial that they possess “cyber warfare troops.” Meanwhile, the United States, sensing its own security vulnerabilities, stood up its newest military Combatant Command, USCYBERCOM, in 2009. This enabled a coordinated defensive and offensive capability in an increasingly digitized world as evident in the U.S.-led Stuxnet and Flame malware operations against Iran in 2010. As a result, both of the prominent digital players in the international community can bring forth debilitating and warlike capabilities. Washington and Beijing even agreed to a spontaneous two-day summit in June to stem the increasingly dangerous game of digital cat and mouse. Unfortunately, the norms guiding the use of cyber forces have yet to be established.

One crucial point lost amid the backdrop of the new digitized battlefield is the lack of Chinese leadership experience both military and political in utilizing key principles of the laws of armed conflict (LOAC). LOAC principles are becoming the foundation and framework for the emerging rules on cyber warfare. Some in China are slowly recognizing this shift. Given the increasingly interconnected, globalized and legally ill-defined nature of cyber technologies, one false move by either the United States or China could steer them into a cyber collision with horrendous conventional consequences.

General Escalation of Force, Proportionality and Rules of Engagement Concepts in War

Jus in bello (just conduct in war) is the set of general laws and principles that govern the way war is fought. It also incorporates the principles of escalation of force (EOF), proportionality, and the rules of engagement (ROE). This was created to promote humane standards in warfare despite the overreaching, destructive nature inherent in war. With the end of WWII, these principles now have been codified with international and customary laws into the Geneva Convention. These embody the modern concept of the law of armed conflict.

U.S. Experience with the LOAC

The U.S. Department of Defense leadership has a vast experience with these principles as they apply to the doctrine of jus in bello. They presently use various rules, approaches, and protocols to abide by the LOAC. Prior to the start of hostilities, military planners will delineate three key principles taken from the LOAC noted earlier: escalation of force (EOF), proportionality, and rules of engagement (ROE). This is to avoid confusion and miscalculation before, during and after hostilities.

The Army’s Escalation of Force Handbook defines EOF as “sequential actions that begin with nonlethal force measures (visual signals to include flags, spotlights, lasers and pyrotechnics) and may graduate to lethal measures (direct action) to include warning, disabling or deadly shots to defeat a threat and protect the force.” Meanwhile, proportionality is military action that is not excessive in relation to the concrete and direct military advantage anticipated. The Army has a uniform Standard Rules of Engagement dictating engagement of force.

Since September 11, U.S. policy makers and military strategists have been provided a tremendous opportunity to finesse those LOAC concepts based on first-hand experience gained in Iraq, Afghanistan, Libya, Guantanamo Bay, on the Korean peninsula and off the Horn of Africa. Each of these situations has spanned a wide range of possibilities in utilizing both cyber and conventional forces. U.S. commanders were required to tailor and adjust these forces to the realities on the ground. This resulted in the integral inclusion of cyber and information warfare training across all military services and senior leaderships. The significance of these experiences has pushed U.S. policy makers to shape frameworks to govern the nebulous and proliferating world of cyber warfare.

The Tallinn Manual and Emerging Cyber Norms

The law-of-armed-conflict principles already established are guiding the discussion and implementation of the emerging rules, doctrines and frameworks that may one day govern the future of cyber warfare. Realizing the need for a LOAC as it applied to the cyber domain, various states, NGOs and individuals have begun to provide their own precepts. Last year, tremendous work and energy by scholars, policymakers and digital leaders from around the world was poured into the Tallinn Manual on the International Law Applicable to Cyber Warfare. This collaborative document provides a starting point to cover the use of force in cyber warfare by state and nonstate actors. However, this document is merely a guiding post and lacks enforcement mechanisms. There is still no globally recognized norm. China has not provided transparency or information regarding their cyber intentions. Despite this, China’s previous views on conventional use of force may offer some clues on future cyber warfare strategies.

The Chinese have not had practical, hands-on experience with escalation of force, proportionality or rules of engagement. The Chinese military has not conducted significant operations since its shellacking in the 1979 border war with Vietnam. Their military has a dearth of expertise in applying these concepts in a real-time threat environment. This inexperience is compounded by the fact that the PRC and PLA leadership define the concepts differently from the United States and others. Because LOAC principles gained from battlefield experience are finding their way into the norms of the cyber domain, the Chinese authorities may be ill-prepared to deal with the pandora’s box of cyber warfare. This mismatch of LOAC experience potentially could cause a miscalculation in any cyber encounter.

Lonnie Henley conducted a study on Chinese escalation management in 2006. He found that Chinese military strategists and theorists segregate EOF and proportionality under their concepts of containment of war (遏制战争 ezhi zhanzheng) and war control (战争控制 zhanzheng kongzhi). Further, he pointed out that Chinese perceptions on war containment and control can be described as the “deliberate actions of war leaders to limit or restrain the outbreak, development, scale, intensity, and aftermath of war” as well as controlling its vertical and horizontal escalation. The Chinese concept of war control is unique in that it seeks a united and focused national effort to maintain the political and military initiative at all cost. The concept of seizing the initiative is not new, and it was even an integral part of Mao Zedong’s war strategy. A recent article in Xinhua by Li Duaguang, a professor at the National Defense University, expounded further on war control by stating that “by preparing for war, one can curb war.” This pull towards seizing the initiative could make Chinese leadership lean too far forward on the side of miscalculation and error. Regrettably, there also has been a dearth of current Chinese discussion on these two principles, so it is difficult to assess Chinese intent in the cyber realm.

Yet, Chinese media reports have filled some of the void with regards to ROE(交战规则 jiaozhan guize). Despite a lack of battle-tested ROE experience, China has linked ROE with cyber warfare and basically has asserted that the United States lacks a legal basis for any unilateral cyber rules of engagement of its own. This is because the Chinese fear that unilateral action by the United States, such as establishing a cyber ROE, would set the stage for future U.S. preemptive action in anticipation of a cyber attack that could target China.

Cyber in China’s Recent Defense White Paper

These pronouncements come at the heels of China’s recently published defense white paper that publicly promulgates its military’s intentions. “Cyber” is mentioned only twice in the entire paper. China did recognize however, that “changes in the form of war from mechanization to informationization are accelerating,” while “major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as . . . cyber space.” China also unequivocally stated in the document that it would “counterattack” if attacked.

Troubling Prospects for U.S.-Chinese Cyber Operations

This is particularly troubling for Chinese and American authorities because it is unclear whether or not they could manage their cyber responses in a measured and proportional way if an unofficial or official outbreak of digital force, intentional or not, were to occur. The severity of this issue is intensified by the lack of official Chinese pronouncements or transparency on their cyber operations. Clandestine cyber units, such as the PLA-sponsored Unit 61398 in Shanghai, operate with destructive global reach, adding a layer of uncertainty to an illicit cyber response.

After a thorough analysis of the defense white paper, it is clear that the Chinese leadership is reticent to articulate their intentions in cyber warfare. For defense purposes, this is troublesome for Washington. There is a variety of political and military reasons for this course of action. Perhaps this Chinese reluctance in setting the guidelines of response stems from the lack of pressure from the United States and other nations. In any case, it is doubtful that the leadership would state a different course of action than its professed desire to conduct only defensive and nonaggressive operations.

Despite this, there is a distinct possibility that if push came to shove, Chinese leadership may be ill-equipped to bring its digital forces to bear or reign in these forces in a responsive, proportional manner once they are released. This is precisely because the Chinese lack LOAC doctrine, training and first-hand experience. The Chinese leadership could make a disastrous miscalculation if it were to mismatch capability or response with the objective or threat at hand, thus risking more confusion and escalation. The recent summit in June may be step toward some sort of digital détente or cyberwar norm. The two states should work to form one sooner rather than later, lest they push each other over the digital edge.

#### Lack of legal clarity is the key internal link --- low transparency results in aggression over Taiwan and makes the US likely to be overaggressive

Austin & Gady 12 (Greg Austin – phD in International Relations, Vice President for the Worldwide Security Initiative, including a leadership role in the institute's work on cybersecurity, is now a Professorial Fellow. Greg has a 30-year career in international affairs, including senior posts in academia and government., Franz Stefan Gady -- M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University., “CYBER DETENTE BETWEEN THE U.S. AND CHINA: Shaping the Agenda, <http://www.ewi.info/system/files/detente.pdf>)

In sum, China is probably engaged in cyber warfare planning for operations against the United States on a very serious level, and possibly more so than for naval or air combat operations against it. At least in relative terms, China’s cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China’s military strategy is highly defensive, but to defend against U.S. operations against China over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind, including through fifth- column policies.

The scale and intensity of United States offensive cyber operations aimed at China on a day-to–day basis may be lower than vice versa, but without access to classified material it would be hard to characterize the difference between the potential disruptive effects of American and Chinese capabilities. This lack of clarity, in an environment of exceedingly low transparency peculiar to cyberspace compared with land, air, sea and space operations, aggravates insecurities on both sides.

The two most urgent tasks for bilateral discussions would therefore appear to be clarifying the relationship between offensive and defensive cyber operations at the strategic and operational levels of war (the thresholds of response), and clarifying the link between these thresholds and traditional notions of strategic nuclear and conventional force deterrence.

#### Nuclear war

Glaser, 11 — Professor of Political Science and International Affairs and Director of the Institute for Security and Conflict Studies at the Elliott School of International Affairs at George Washington University (Charles, “Will China's Rise Lead to War?: Why Realism Does Not Mean Pessimism”, Foreign Affairs, March/April 2011, lexis)

ACCOMMODATION ON TAIWAN? THE PROSPECTS for avoiding intense military competition and war may be good, but growth in China's power may nevertheless require some changes in U.S. foreign policy that Washington will find disagreeable--particularly regarding Taiwan. Although it lost control of Taiwan during the Chinese Civil War more than six decades ago, China still considers Taiwan to be part of its homeland, and unification remains a key political goal for Beijing. China has made clear that it will use force if Taiwan declares independence, and much of China's conventional military buildup has been dedicated to increasing its ability to coerce Taiwan and reducing the United States' ability to intervene. Because China places such high value on Taiwan and because the United States and China--whatever they might formally agree to--have such different attitudes regarding the legitimacy of the status quo, the issue poses special dangers and challenges for the U.S.-Chinese relationship, placing it in a different category than Japan or South Korea. **A crisis** over Taiwan **could** fairly **easily escalate to nuclear war**, because each step along the way might well seem rational to the actors involved. Current U.S. policy is designed to reduce the probability that Taiwan will declare independence and to make clear that the United States will not come to Taiwan's aid if it does. Nevertheless, the United States would find itself under pressure to protect Taiwan against any sort of attack, no matter how it originated. Given the different interests and perceptions of the various parties and the limited control Washington has over Taipei's behavior, a crisis could unfold in which the United States found itself following events rather than leading them. Such dangers have been around for decades, but ongoing improvements in China's military capabilities may make Beijing more willing to escalate a Taiwan crisis. In addition to its improved conventional capabilities, China is modernizing its nuclear forces to increase their ability to survive and retaliate following a large-scale U.S. attack. Standard deterrence theory holds that Washington's current ability to destroy most or all of China's nuclear force enhances its bargaining position. China's nuclear modernization might remove that check on Chinese action, leading Beijing to behave more boldly in future crises than it has in past ones. A U.S. attempt to preserve its ability to defend Taiwan, meanwhile, could fuel a conventional and nuclear arms race. Enhancements to U.S. offensive targeting capabilities and strategic ballistic missile defenses might be interpreted by China as a signal of malign U.S. motives, leading to further Chinese military efforts and a general poisoning of U.S.-Chinese relations.

#### We solve- our adherence to LOAC is modeled globally. OCO ambiguity is the biggest internal link

Bradbury 11 (Steven Assistant Attorney General for the Office of Legal Counsel, 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.13

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.

One final admonition I’ll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committees — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

#### Congressional restrictions on OCOs send a global signal of cyber leadership that solves reckless use of OCOs

Bastby 12 (Judy, Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee, 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 Congress 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.

#### Action now is key – failure will result in a rapidly created worse legal system that non uniques all their offense

SCHAAP 09 Major – Air Force, the Directorate of Legal Services, Headquarters Air Command, RAF High Wycombe, United Kingdom. JD Cal Western, LLM George Washington, Former Deputy Staff Judge Advocate, Lackland [Major Aire J. Schaap, CYBERLAW EDITION: CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW, Air Force Law Review, 64 A.F. L. Rev. 121]

IX. CONCLUSION

Nothing in international law explicitly prohibits cyber warfare operations. However, legal limitations surely exist with regard to their application. Also, cyber warfare operations have the potential of constituting a use of force or a violation under the law of war.

Cyber warfare operations offer a variety of methods to impact an adversary's ability to conduct war. They may enable a state to infiltrate an adversary's network, acquire files, spread misinformation, or introduce weaknesses into an adversary's systems. Cyber warfare operations may also make it possible for a state to take control of an adversary's network for the purpose of temporarily or permanently disabling it or affecting the infrastructure it supports. n344 Additionally, cyber warfare operations have the potential of depriving an adversary of essential infrastructure that supports military actions, such as communication satellites. One advantage of cyber warfare operations is that they will often achieve their desired results with less collateral damage than traditional warfare, such as, disabling an electrical grid by accessing its network in lieu of bombing the power plant. n345

Despite the fact that cyber warfare operations have the potential of limiting collateral damage during times of hostilities, they pose several risks to states that may employ such warfare. One example would be the potential escalation of minor hostilities into a full blown armed conflict. For example, State A, having received specific evidence establishing that State B was behind DoS attacks against State A's government, declares the acts an unlawful use of force and orders an aerial bombing campaign against State B's communication facilities, the source of the attack. State B may in turn declare the acts of State A as acts of war and launch missiles into State A. In this scenario who is to blame? Did anyone actually violate international law?

One of the greatest challenges of law is keeping up with the advancement of technology. n346 The international community has often struggled to implement standards of conduct in a timely manner regarding the advancement of weaponry. n347 In the past, when new technologies emerged, in an effort to avoid war or minimize human suffering when conflicts occur, states drafted rules resulting in, for example, treaties restricting biological, chemical, and laser weapons. n348 In March 2006, Nikolai Kuryanovich, a member of the Russian Duma, noted in a letter to an ultranationalist hacker group known as the Slavic Union that, "In the very near future many conflicts will not take place [\*173] on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers . . . ." n349 I contend that the future Mr. Kuryanovich discusses is now, and that now is the time for states to determine what is and is not permitted under international law in relation to cyber warfare operations. Failure to do so now may result in overly restrictive, reactionary regulations in response to a cyber Pearl Harbor-like attack, rather than a well thought out, proactive, structured approach.

#### 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.

#### Regulation and arms control solves nuclear and kinetic war

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)

10.2.1 Direct Approaches Based on Traditional Arms Control

What purposes could be served by a regulatory regime for cyberattack? Traditional arms control theory generally indicates that three broad purposes could be served in principle, presuming that the restrictions of the regime are observed by all signatories:

• Reducing the likelihood that conflict will occur. Confidence-building measures—arrangements in which signatory parties agree to refrain from or to notify other signatories prior to conducting certain activities that might be viewed as hostile or escalatory or to communicate directly with each other during times of tension or crisis—are explicitly intended to reduce the likelihood of conflict due to accident or misunderstanding. In addition, agreements to eschew the use of cyberattack may have some value in reducing the likelihood of kinetic conflict in those cases in which cyberattack is a necessary prelude to a kinetic attack.

• Reducing the destructiveness of any conflict that does occur. Limitations on targeting cyberattack weapons could prevent damage to the prohibited entities, presuming that the scope of a cyberattack can be delimited with confidence. Moreover, limiting damage to those entities might prevent escalation from occurring—and such escalation could include escalation to kinetic or even nuclear conflict. Reducing destructiveness might also facilitate a more rapid cessation of cyberhostilities.

• Reducing financial costs. Limitations on acquisition of weapons for cyberattack would not have a significant impact on financial costs, simply because these weapons are so inexpensive in the first place. Nor would a particular adversary’s agreement to refrain from conducting cyberattack relieve the United States from needing to defend against other nations or subnational entities that could use such weapons.

Given the possibilities for cyberattack to disrupt national economies or to distort the activities of individual companies as well (especially large companies that are very important to a nation), a regulatory regime for cyberattack might also reduce the likelihood of economic warfare using this military tool.