Spring 2014

Cyber Power Restrained: How Strategic Culture Inhibits the Integration of Cyber Weapons by the United States Military

David Matthew Bisson
Bard College, db0611@bard.edu

Cyber Power Restrained:

How Strategic Culture Inhibits the Integration of Cyber Weapons by the United States Military

Senior Project submitted to

The Division of Social Studies

Of Bard College

By

David Bisson

Annandale-on-Hudson, New York

April 2014

Acknowledgments

I would like to thank the Department of Political Studies at Bard College, in particular its knowledgeable professors and students, for creating an intellectual environment conducive to the production of this paper. I enjoyed some of my most cherished and challenging academic moments in the Department. I therefore owe my undergraduate education to all of those individuals who helped me grow, both as a scholar of politics and as an individual.

I am grateful to Martin C. Libicki for the initial guidance he provided on my research and for sending me a copy of his lectures early on. He truly lit the spark under my research efforts.

I cannot express enough gratitude to Christopher McIntosh, who provided constant encouragement as my primary thesis adviser. He shared pieces of insight around every turn and challenged me to dig deeper into my research. I am forever indebted to him for what he has taught me and am thankful for having had the experience to work with him.

Finally, I would like to thank my family for their constant love, inspiration, and encouragement. I am eternally grateful to my brother Jonathan and mother Lynda, who gave feedback on my arguments, read my drafts, and supported me every step of the way. I would also like to thank Lea for always believing in me. Without their support, this paper would not have been possible.

ABSTRACT

This article seeks to reconcile the support status of cyber power in the United States military with the seriousness of the cyber threat confronting the nation. It rejects the argument that cyber weapons are not useful and are not traditional "weapons" by drawing parallels between cyber power and military force in the physical domains, as well as revealing how some of the most prominent issues in cybersecurity are political and not technological in nature. The article proposes strategic culture as an alternative explanation for U.S. cyber power's current status. By studying the case studies of American air and space power, the analysis arrives at four factors that characterize the U.S. military's integration of new technologies: 1) the initial use of new technologies to provide support to the services, 2) the importance of public interest in driving or constraining integration, 3) the effect a national crisis can have on helping the military overcome constraints against integration, and 4) the influence of external conflict on the military's integration of new technologies. These findings together constitute a model which attributes the current status of cyber power to a history of dependence, public ignorance and lack of concern, and the absence of a "Cyber Pearl Harbor." Acknowledging this, a cyber attack or cyber war against the United States has the best chance of changing the current status of American cyber power.

Introduction

Today, people regard "cyberspace"—a digital realm encapsulating users' transactions on computers and across internet and communication technologies (ICTs)—as a medium in which everyone can invent new identities, communicate freely, and participate in a globalized world. But cyberspace is not entirely safe. Hacking has evolved into more nuanced forms of penetration, and terrorist networks, cyber criminals, and rogue states can now target nations' critical infrastructures, the functions of which are dependent on computer technology.

As a result of these developments, the U.S. military has established a presence in cyberspace. In 2006, the Joint Chiefs of Staff (JCS) defined the military's interest in cyberspace as emblematic of a new doctrine of warfare. Network-centric operations (NCOs), or the use of ICTs to build a command's "shared awareness" of the battlefield, embody the point that computers can help generals understand a battlefield, issue orders, and confront some of the challenges posed by modern warfare. [1] The U.S. military realizes this strategic utility of ICTs, not to mention how attackers can use computer technology to attack the vast network of commercial companies on which it depends for communications and logistics support. [2] Cyberspace has even evolved into an independent military domain in need of its own deterrence mechanisms. As a result, the U.S. military has established a presence in the cyber sphere.

Three examples demonstrate the cyber threats confronting the U.S. military. The first is an example of cyber attacks being used to disrupt civilian infrastructure, which in turn adversely affects the military. Imagine that a type of malware is successfully used to disrupt computers

---

[1] Clay Wilson, "Network Centric Operations: Background and Oversight Issues for Congress," *Congressional Research Service*, published March 15, 2007, accessed March 2, 2014, http://www.fas.org/sgp/crs/natsec/RL32411.pdf, 1.

[2] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham: Syngress, 2011), 15.

that monitor the transferal of oil at a refinery. Those computers might not be able to process new orders, causing oil shortages around the world. This would spell trouble for the U.S. military. Not only would it receive less oil for its vehicles, but the "military-industrial complex" would come to a halt when private contractors could no longer afford to transport their goods and services. Such an attack would therefore diminish the ability of the U.S. military to project power at home and abroad.

The second example, which goes back to the Cold War, involves cyber attacks being used as military acts in times of war. In January 1982, a Trans-Siberian gas pipeline exploded unexpectedly. Many reports assert the CIA caused the explosion by inserting a Trojan virus into the software that managed the pipeline's pressure.[3] This incident demonstrates that cyber weapons can produce "real world" effects similar to those of traditional weapons. It also illustrates the converse: kinetic attacks are like cyber attacks in that both render something inoperable. The justification for taking out a military target, such as an oil pipeline, is that the target will be eliminated. Casualties and/or collateral damage are secondary effects. In this instance, just as cyber weapons can render a pipeline inoperable by corrupting pressure sensors, bombs can do the same by destroying the pipeline altogether.

Lastly, a cyber attack on U.S. military networks is an example of cyber weapons being used to disrupt the military's functionality. Given the prevalence of NCOs, a cyber attack on a military network would actually have more far-reaching effects than a kinetic attack. Orders might not be issued. Supplies might not arrive. The military's leadership might receive false or outdated information. All of these would place American soldiers in danger. In an age where

[3] George Kostopoulos, *Cyberspace and Cybersecurity* (Boca Raton: Taylor & Francis Group, LLC, 2013), 117.

information is crucial to winning a war, manipulating a combatant's intelligence can mean the difference between victory and defeat.

Interestingly, Stuxnet fits all three classifications. Discovered in June 2010, Stuxnet is responsible for having damaged the centrifuges at an Iranian nuclear enrichment plant located in Natanz.[4] The attack was so devastating that it allegedly set the entire Iranian nuclear program back by two years.[5] In this sense, Stuxnet was a military attack that transcended the digital-kinetic divide and undermined Iran's ability to produce a nuclear weapon. Stuxnet also disrupted the Iranian military insofar as the attack forced it to reallocate funds in an effort to resume its nuclear program, not to mention postponed its acquisition of certain weapons which could figure largely into all of its future operations. At the same time, however, some believe Stuxnet helped delay the startup of Iran's Bushehr's nuclear power plant,[6] which today is now generating electricity for civilian use.[7] As a result, Stuxnet also disrupted civilian infrastructure by delaying the production of nuclear power for non-military consumption.

In response to the threats explained above, the American armed services have militarized cyberspace. No action captures this better than the creation of United States Cyber Command (USCYBERCOM). The sub-unified command pursues a two-pronged mission. First, it protects, guides, and defends the DoD's information networks on a daily basis.[8] Second, it uses its

---

[4] Mark Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant," *Christian Science Monitor*, published November 16, 2010, accessed April 25, 2014, http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

[5] Peter Bright, "Stuxnet apparently as effective as military strike," *Ars Technica*, published December 16, 2010, accessed April 25, 2014, http://arstechnica.com/tech-policy/2010/12/stuxnet-apparently-as-effective-as-a-military-strike/.

[6] Mark Clayton, "Stuxnet malware is 'weapon' out to destroy…Iran's Bushehr nuclear plant?," *Christian Science Monitor*, published September 21, 2010, accessed April 25, 2014. http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

[7] "Iran to launch second stage of Bushehr nuclear plant," *PressTV*, published March 1, 2014, accessed April 25, 2014, http://www.presstv.com/detail/2014/03/01/352797/iran-to-launch-2nd-stage-of-bushehr-plant/.

[8] "US Cyber Command," *U.S. Army Cyber Command*, accessed November 26, 2013, http://www.arcyber.army.mil/org-uscc.html.

resources to "coordinate DoD operations providing support to military missions… [as well as] prepare to, and when directed, conduct full spectrum military cyberspace operations."[9] By full-spectrum cyber operations, the DoD means the full range of cyber weapons that can be used to support military functionality and its networks' viability.[10]

Curiously, the mission of USCYBERCOM does not fully address the seriousness of the cyber threat confronting the United States. The Department of Defense has ample financial resources and political will, so it should respond rationally and grant cyber power more operational autonomy, i.e. enable CYBERCOM to launch attacks both offensively and defensively against targets in cyberspace using tactics and strategies whose formulation it oversees with an appreciable degree of non-interference from the other services. But the DoD has not, which begs the question: If cyber technology constitutes a real threat to the United States, why is the U.S. military restraining cyber power to support functions only?

In this paper, I seek to answer the question, "Why does the United States military not grant cyber power greater operational autonomy?" My conclusion is the organizational culture of the U.S. military is responsible. I begin by explaining the conventional wisdom, which maintains that the U.S. military restrains its use of cyber power because cyber technology is too ambiguous for cyber weapons to be useful or even constitute "weapons" in a traditional sense. This technologist argument understands technology as ahistorical and static and asserts that four issues unique to cyberspace—casualties, proportionality, signaling, and attribution—preclude a further integration of cyber power. I refute these claims by demonstrating how these problems

[9] Ibid.
[10] U.S. Department of Defense, *Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates*, published July 29, 2011, accessed November 26, 2013, http://www.gao.gov/assets/100/97674.pdf, 2.

apply to conventional weapons already adopted by the military. I also illustrate how the nature of many of these problems is political, not technological, in nature.

In the second section of my paper, I present my main argument. Militaries are always adopting new technology, and this process can only be understood by going beyond the technology in question to include changes that reflect the overall culture of the military. Subsequently, the U.S. military's strategic culture—its beliefs, expectations, and values that inform how it pursues its objectives[11] —is a better explanation of why the U.S. military has not integrated U.S. cyber power further.

The notion of strategic culture carries significant implications for understanding U.S. cyber power. It acknowledges, among other things, the importance of history with respect to military change.[12] The U.S. military has a unique history that informs its strategic actions. U.S. cyber power is not an ahistorical variable of technology but rather a process of military change, informed by the historical developments, behaviors, and actions of the American armed services as an organization.

I examine U.S. military strategic culture through two case studies—U.S. air power and space power—in the third section of my paper. These cases are important because, like cyber power, they produced technology booms in the United States, helped constitute entirely new warfighting domains for the U.S. military, and revolutionized modern military affairs. These cases reveal four important commonalities: the initial support status of new technologies, the role of popular interest in motivating (or preventing) change, organizational change following a national crisis, and the centrality of external conflict. I end the section by synthesizing these elements together into a model for military technological integration in the United States.

---

[11] Alastair Iain Johnston, "Thinking about Strategic Culture," *International Security* 19, no. 4 (1995): 34.
[12] Ibid.

In the fourth section, I use this model to examine U.S. integration of cyber power. I demonstrate how each of the four components work against further integration of cyber technology on the part of the U.S. military at this time. I then cite three developments—the increasing variety of potential applications of cyber weapons, the unlikelihood of a cyber warfare convention, and the decreasing costs of cyber capabilities—to illustrate a trend by which actors have a growing incentive to launch a cyber attack against the United States. While such an attack may never occur, it is the most likely way the U.S. military would grant American cyber power greater operational autonomy. Finally, I conclude by showing how my model for technological integration relates to the military's current use of other new technologies.

The Technologist Argument

The technologist argument asserts that the U.S. military has not given more operational autonomy to American cyber power because cyber technology is ambiguous. According to this argument, the U.S. military uses cyber power only as means of support because cyber weapons cannot explode and cannot kill people. If they lack kinetic force to blow up a military target and cannot cause casualties in the process, the U.S. military has no use for these types of weapons on the battlefield. This argument further argues that notions of "intention", "identity", and "damage" are fundamentally variable in cyberspace. An actor cannot directly cause casualties, determine proportionality of response, signal its intentions, or confidently attribute the source of an attack, all of which one can allegedly do with conventional and nuclear weapons. As such, these issues reveal that cyber weapons are not actually "weapons" and are not military useful.

In the following section, I argue the technologist argument is inadequate for explaining the status of U.S. cyber power. First, I explain each of the four problems discussed above. I then

offer a rebuttal to each explanation by drawing parallels to conventional weapons or revealing the political and *not* technological nature of each problem.

CASUALTIES

Most IR scholars and U.S. military leaders cite the alleged inability to inflict casualties as a reason why cyber power continues to be tied to the traditional services. One of the lead proponents of this viewpoint is Thomas Rid. Rid is well-respected in the cyberwar debate. Perhaps the greatest source of his fame has been the publication of *Cyber War Will Not Take Place*, in which he questions the notion of "violence" in cyberspace.

It is important here to propose a working definition of "violence." Willem de Haan understands violence as "an act of physical hurt deemed legitimate by the performer and illegitimate by (some) witnesses."[13] For an act to be violent, physical harm must be transferred between the attacker and victim. One type of violence, "political violence," is undertaken by a group of individuals who share some political motivation for their actions.[14] This often takes the form of an act which threatens to change or undermine the legitimacy of a political system.[15] Political violence therefore aims to disturb certain social relations and associated ways of life.[16]

Rid argues that political violence in cyberspace is different than in the real world because attackers can cause casualties only indirectly.[17] Cyber attacks cannot *directly* cause casualties because the act of force (the cyber attack) and the response (human death) are located in two different media: the former in cyberspace, and the latter in the real world. Cyber operations

---

[13] Willem de Haan, "Violence as an Essentially Contested Concept," in *Violence in Europe: Historical and Contemporary Perspectives*, ed. Sophie Body-Gendrot and Pieter Spierenburg (New York: Springer, 2008), 30.
[14] Perry Mars, "The Nature of Political Violence," *Social and Economic Studies* 24, no. 2 (1975): 228.
[15] Ibid.
[16] Brandon Hamber, *Transforming Societies After Political Violence: Truth, Reconciliation, and Mental Health* (New York: Springer, 2009), 22.
[17] Raffaello Pantucci, "Cyber War Will Not Take Place," *Rusi Journal* 158, no. 6 (2013): 106.

negate the symbolism of the human body as it relates to causing and receiving violence.[18] This means that cyber weapons are not violent, which invalidates the possibility of the U.S. military integrating cyber power beyond its current non-violent support functions.

Notwithstanding the praise it has received, Rid's argument is flawed chiefly because he employs a definition of violence that, by only recognizing acts that directly cause damage to the body, is far too narrow in today's world. Jun Osawa notes, for instance, that the lethality of cyber attacks rests in their ability to cause systems that monitor national critical infrastructure to malfunction.[19] By attacking electrical power grids, air traffic control towers, and/or industrial plants, malicious actors in cyberspace can precipitate events that could result in death.[20] This may be an indirect means of causing casualties, but it is no less of a potential concern.

By dismissing the indirect lethality of cyber weapons, Rid emphasizes the *method* of violence at the expense of its *consequences*.[21] This minimalist conception of violence misreads today's world. Rid would benefit from analyzing violent acts with regards to their effects, both direct and indirect.[22] By accepting this framework, he and other scholars could understand how and why the effects of one type of cyber attack can vary depending on its target.[23] Additionally, they could also see how violence can be committed against things and then passed to people,[24] which reflects the dangers of a cyber attack launched against national critical infrastructure.

---

[18] Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 15.
[19] Jun Osawa, "Is Cyber War Around the Corner? Collective Cyber Defense in the Near Future," *Brookings*, published November 2013, accessed February 18, 2014, http://www.brookings.edu/research/opinions/2013/11/12-cyber-defense-us-japan-alliance-osawa.
[20] Ibid.
[21] Michael Turner, "Is There Such a Thing as a Violent Act in Cyberspace?," *International Security and Intelligence Summer School 2013, Pembroke College, and the University of Cambridge*, accessed February 18, 2014, http://www.pem.cam.ac.uk/wp-content/uploads/2013/04/Is-there-such-a-thing-as-violence-in-cyberspace.pdf, 1.
[22] Larry Ray, *Violence and Society* (New York: SAGE Publications Ltd., 2011), 9.
[23] Michael Turner, "Is There Such a Thing as a Violent Act in Cyberspace?," 3.
[24] "Violence," *Oxford Dictionary*, accessed February 18, 2014, http://www.oxforddictionaries.com/us/definition/american_english/violence.

But even beyond conceptions of violence, modern warfare as a phenomenon is shifting away from violence more generally. Since the end of the twentieth century, violent interstate wars conducted on discrete battlefields have been replaced by irregular warfare (IW), low-intensity conflicts that are asymmetric in nature and which may involve non-state combatants hiding among civilian populations for protection and support.[25] These operational constraints pose serious challenges to the U.S. military. On the one hand, its mission has not changed: it still needs to eliminate those who threaten the security of the U.S. But on the other hand, any application of force threatens to result in significant collateral damage, which could undermine the military's legitimacy.[26] Balancing these two objectives is no small challenge.

In response, the American armed services have done two things. First, they have started to use "smart" weapons as a means to counter the liability posed by human soldiers. Command and control (C2), the ability of a commanding officer/headquarters to coordinate operations in the battlefield, is vitally important in war.[27] But by relying on humans, who can die in combat or fail to fulfill their orders, military organizations are needlessly risking the success of their missions when they could use more dependable, more resilient machines instead.[28] Warfare is becoming too fast and complex for humans, and weapon systems are cheaper to replace than human soldiers, anyway.[29] Subsequently, the U.S. military is now casualty-averse for strategic purposes.[30] War threatens to kill too many soldiers, which translates into a decline in public

---

[25] Richard L. Scott, *Conflict Without Casualties: Non-Lethal Weapons in Irregular Warfare* (Monterey: Naval Postgraduate School, 2007), 21.
[26] Ibid.
[27] Carl H. Builder, Steven C. Bankes, and Richard Nordin, *Command Concepts: A Theory Derived From Practice of Command and Control* (Santa Monica: RAND Corporation, 1999), xiii-xiv.
[28] Thomas K. Adams, "Future Warfare and the Decline of Human Decisionmaking," *Parameters* 41 (2011): 8.
[29] Mark Gubrud, "US Killer Robot Policy: Full Speed Ahead," *Bulletin of the Atomic Scientists*, published September 20, 2013, accessed February 19, 2014, http://thebulletin.org/us-killer-robot-policy-full-speed-ahead.
[30] Chukwuma Osakwe, "Non-Lethal Weapons and Force-Casualty Aversion in 21st Century Warfare," *Journal of Military and Strategic Studies* 15, no. 1 (2013): 2.

support for any war effort.[31] Acknowledging this, by using autonomous weapon systems, the U.S. military stands to use its resources more economically, protect its human soldiers, and enhance its ability to wage war over extended periods of time.

Second, the U.S. military is now investigating the use of non-lethal weapons (NLWs). NLWs refer to non-lethal chemical, electromagnetic, and kinetic devices that law enforcement and military personnel can use to undermine an enemy's aggression and/or lethality with minimal risk of collateral damage.[32] These weapons range from crowd-control instruments, such as pepper spray canisters, deployable nets, and batons,[33] to more sophisticated systems like the Long Range Acoustic Devices (LRADs), which emits a high-pitched tone capable of producing hearing loss at up to 500 yards away.[34]

The U.S. military clearly has a number of potential NLWs at its disposal, not the least of which is cyber weapons. With the creation of USCYBERCOM, Air Force Major General William Lord envisioned cyber power as the first step towards fighting non-kinetic wars.[35] The U.S. military could feasibly use cyber weapons to scramble other countries' banking systems and possibly preempt armed conflict.[36] Cyber weapons could therefore be used to replace guns and bombs, making warfare less bloody.

Rid's argument is an inaccurate explanation of why the U.S. military has not integrated cyber power further. As explained above, cyber weapons do have the potential to cause

---

[31] Yagil Levy, "The Tradeoff between Force and Casualties: Israel's Wars in Gaza, 1987-2009," *Conflict Management and Peace Science* 27, no. 4 (2010): 388.
[32] Chukwuma Osakwe, "Non-Lethal Weapons and Force-Casualty Aversion in 21st Century Warfare," 6.
[33] National Security Research, Inc., *Department of Defense Non-Lethal Weapons and Equipment Review: A Research Guide for Civil Law Enforcement and Corrections*, no. 200516, published June 19, 2003, accessed February 20, 2014, https://www.ncjrs.gov/pdffiles1/nij/grants/200516.pdf.
[34] Richard L. Scott, *Conflict Without Casualties*, 36.
[35] Sebastian Sprenger, "Air Force General Emphasizes Focus on Nonkinetic Warfare," *Federal Computer Week*, published September 6, 2007, accessed February 20, 2014, http://fcw.com/articles/2007/09/06/air-force-general-emphasizes-focus-on-nonkinetic-warfare.aspx.
[36] Ibid.

casualties via indirect means and can therefore be "violent" in a traditional sense. But this is beside the point. Autonomous weapon systems are replacing human soldiers, thereby eroding the symbolism of the human body in violence. Also, war is generally becoming less violent in general, as evidenced by the U.S. military's growing interest in NLWs. Cyber weapons are therefore neither anomalous nor violent. Rather, they are one manifestation of a new paradigm of warfare in which conflicts are increasingly automated and (eventually) non-kinetic in nature.

PROPORTIONALITY

Proportionality of response states that any incidental damage, destruction, or death that may be caused to civilian populations as a result of a military operation should not exceed that mission's strategic utility.[37] It is a staple of the law of armed conflict (LOAC), relating in particular to *jus ad bellum*, the legal principles which help states decide whether to go to war, and *jus in bello*, or states' non-right to use unlimited force in war.[38] These notions constitute a large part of just war theory, which upholds a number of normative principles, including proportionality, in an attempt to constrain states and protect innocent life in war.

Some scholars maintain that proportionality is impossible to determine in cyberspace. They do so by extending Rid's argument explained above. The effects of a cyber attack vary depending on the target system.[39] In most cases, the exact make-up of a target is not known beforehand. This means that a retaliator can only determine proportionality on an *ex post facto* basis when responding to a cyber attack.

---

[37] Harold Hongju Koh, "International Law in Cyberspace," *U.S. Department of State*, published September 19, 2012, accessed October 19, 2013, http://www.state.gov/s/l/releases/remarks/197924.htm.
[38] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly Media, Inc. 2012), 31.
[39] Paul A. Walker, "Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine," *National Security Law Brief* 1, no. 1 (2011): 40.

But the problem runs even deeper than that given the ongoing uncertainty regarding what should constitute "damage" in cyberspace. The effects of most cyber attacks are digital and therefore do not affect the "real" world. Some feel this means that cyber weapons cannot cause actual damage. Furthermore, a cyber attack's digital effects are neither immediately nor publically visible to either the attacker or to any third parties.[40] Only the victim knows the exact effects of an attack. This ambiguity could incentivize victims to exaggerate the level of damage in an attempt to justify a disproportionately high retaliatory act, thereby ignoring proportionality and intentionally escalating a conflict.

The technologist argument maintains that proportionality in cyberspace is difficult because cyber attacks are non-traditional operations whose effects are visible only to the victim and depend on the target system, the details of which an attacker never fully knows. These factors make both disproportionate responses and inadvertent escalation likely. If cyber weapons cannot be used proportionately, the argument goes, they should not be used at all. Subsequently, the U.S. military has allegedly refrained from integrating cyber power further.

Those who argue that the proportionality is difficult to uphold in cyberspace miss a larger point: it is difficult to determine proportionality in *any* domain. Militaries concerned with proportionality must strike a delicate balance between protecting innocence and wreaking destruction, yet there is no standard legal framework by which they can do this.[41] Instead militaries must subjectively define important issues, such as who constitutes a "civilian" in IW, when determining proportionality. Additionally, proportionality is an ambiguous principle. What constitutes a "military advantage," for example, is unclear given the variance of time and

[40] Jason Andress and Steve Winterfeld, *Cyber Warfare*, 233.
[41] Jonathan Wallace, "Proportionality and Responsibility," *The Ethical Spectacle*, published August 2006, accessed February 13, 2014, http://www.spectacle.org/0806/proportionality.html.

space as they relate to military action. Together, these uncertain factors make proportionality dependent on the strategic calculations of the U.S. military as a subjective actor.

An example is useful. Over the past few years, the United States' has used unmanned aerial vehicles (UAVs) or "drones" to target and kill the personnel associated with Al Qa'ida and other terrorist cells.[42] Over the course of their deployment, U.S. drone attacks have caused hundreds if not thousands of civilian casualties,[43] which has raised questions of proportionality. In response, Obama changed the rules of the game: he redefined "combatants" as all military-age men within a combat zone.[44] Obama manipulated the definition of "combatants" to get around proportionality in pursuit of the United States' security interests. This demonstrates that the principle is fundamentally weak and can in fact be skewed to fit actors' subjective goals.

Proportionality of response is difficult to uphold in any domain. The principle is plagued by ambiguous components, which has allowed politicians to manipulate language in an attempt to get around it. Proportionality has no objective grounding. Subsequently, just as the U.S. military can apply proportionality subjectively at sea or on land, it can do so in cyberspace.

SIGNALING

Another factor that technologists use to explain why the U.S. military has not given more operational autonomy to cyber power is the difficulty of signaling in cyberspace. Signaling is a crucial part of war, for every action in combat communicates a message to an adversary. For

---

[42] Tom Cohen, "When Can a Government Kill Its Own People?," *CNN Politics*, published February 11, 2014, accessed February 13, 2014, http://www.cnn.com/2014/02/10/politics/us-killing-americans/.
[43] "U.N. Rights Chief "Seriously Concerned" Over U.S. Drone Strikes in Pakistan, Echoed by Iran," *UN Watch*, published June 19, 2012, accessed February 13, 2014, http://blog.unwatch.org/index.php/2012/06/19/u-n-rights-chief-seriously-concerned-over-u-s-drone-strikes-in-pakistan-echoed-by-iran/.
[44] Joe Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *The New York Times*, published May 29, 2012, accessed February 13, 2014, http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?_r=3&pagewanted=all&.

example, the use of military force articulates the threat that, unless its enemy stops, one will continue to employ or escalate the violence. On the flip side, signaling is just as important for conflict management. As noted by Thomas C. Schelling, classic game theory involves players using signals to reveal their intentions.[45] This helps players get to know one another, knowledge which they can use to avoid escalating a conflict.[46] But it is not that easy. For signaling to work in any scenario, both actors must not only agree to what constitutes a signal,[47] but they must also *interpret* each signal the same way. Signaling is therefore a delicate and context-dependent act.[48]

Cyberspace is cited as a remarkably difficult medium for signaling. It is an intrinsically "noisy" environment,[49] mainly because of the difficulty associated with attributing the source of a cyber attack.[50] This becomes especially tricky with "third party" actors, who may, if they launch attacks of their own, complicate the process of signaling between two actors.[51]

Furthermore, even if it is clear that an enemy has attacked, some feel that signaling in cyberspace is still difficult given the fact that a cyber signal can be interpreted more than one way.[52] As an example, the United States' decision to form USCYBERCOM potentially conveys multiple messages. The U.S. might be signaling its resolve to respond to cyber attacks, its fear of being attacked, or its determination to use cyber capabilities offensively against others.[53] Other states might feel compelled to launch preemptive cyber attacks against the U.S. in an

---

[45] Thomas C. Schelling, "The Strategy of Conflict: Prospectus for a Reorientation of Game Theory," *The Journal of Conflict Resolution* 2, no. 3 (1958): 204.
[46] Ibid.
[47] Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), 62.
[48] Mason Rice, Jonathan Butts, and Sujeet Shenoi, "A Signaling Framework to Deter Aggression in Cyberspace," *International Journal of Critical Infrastructure* 4 (2011): 61.
[49] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 114.
[50] Ibid.
[51] Ibid., 133.
[52] Stephen J. Cimbala, "Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble?," *Strategic Studies Quarterly* 5, no. 1 (2011): 123.
[53] Martin C. Libicki, *Crisis and Escalation in Cyberspace*, 66.

attempt to prevent it from realizing its cyber ambitions. This would encourage the U.S. to retaliate, possibly leading to a cyber war borne out of misunderstanding and poor signaling.

In cyberspace, it is difficult to signal one's intentions. An actor such as the U.S. has a difficult time determining whether it is signaling to the appropriate cyber actor and whether it is sending the right message. Given these difficulties, the U.S. military under the technologist argument lacks an incentive to broaden its use of cyber power.

However, the problems associated with signaling in cyberspace apply to all instances of signaling. In an effort to issue a credible threat to an adversary and force it to back down from conflict, actors in any domain may use "costly signals"—actions that raise the likelihood of war.[54] Examples of costly signals include mobilizing one's troops or conducting a display of force. Both reveal the defender's resolve to respond to an attack.[55]

Using costly signals is dangerous. They are subjectively issued and interpreted and can therefore be misinterpreted. For example, during the Cold War, the U.S. periodically increased its defense spending to signal its commitment to deterring the spread of worldwide communism. But the Soviet Union interpreted this merely as a reflection of the needs of the United States' economy.[56] Even in a binary international system, actors can misinterpret signals.

In today's world, third parties can complicate signaling in all domains, including those which involve nuclear weapons. For example, researchers at the Institute for Foreign Policy Analysis have warned about the possibility of "catalytic warfare," in which third-party actors

---

[54] Vesna Danilovic, *When Stakes Are High: Deterrence and Conflict Among Major Powers* (Ann Arbor: University of Michigan Press, 2002), 155.
[55] Paul K. Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2 (1999): 31.
[56] Robert Jervis, "Signaling and Perception: Drawing Inferences and Projecting Images," in *Political Psychology*, ed. by Kristen Renwick Monroe (Mahwah: Lawrence Erlbaum Associates, Inc., 2002), 302.

skew the signals of two major powers and start a nuclear war between them.[57] The spoiling influence of third party actors on crisis management therefore extends beyond cyberspace.

Signaling is difficult in any domain. Whenever two actors are trying to signal their intentions to one another, signals can be misinterpreted or skewed by third parties, possibly escalating a conflict into war. Acknowledging this, signaling is not a technological problem but a political issue characteristic of most conflicts across all domains.

ATTRIBUTION

For the U.S. military to wage war, it must clearly define its enemy. But this is problematic in the cyber realm. Much of this difficulty arises from the layered architecture of the attribution problem. On the *technical* layer, analysts must identify that an attack has occurred and trace the infected data back to an Internet Protocol (IP) address, a unique identifier which serves as a destination code.[58] Attributing a cyber attack therefore requires a fair amount of forensic work.

But even if an attack can be traced back to an IP address, the identity of an offender may still be elusive. For instance, if admins are able to trace an attack back to the IP address of a foreign government, this could mean that government employees are responsible, or that hackers have hijacked the government's network to confuse their victims.[59] Clearly, attributing an attack at the *social* level, or where a human user can be identified, is a complex process.[60]

The third and final layer of the attribution problem is the *political*. This level is partially a consequence of the Internet's decentralized nature. States could easily issue new laws and

---

[57] Jacquelyn K. Davis, et al., "Updating U.S. Deterrence Concepts and Operational Planning: Reassuring Allies, Deterring Legacy Threats, and Dissuading Nuclear 'Wannabes,'" *Institute for Foreign Policy Analysis*, published February, 2009, accessed February 16, 2014, http://www.ifpa.org/pdf/Updating_US_Deterrence_Concepts.pdf.
[58] Thomas Rid, *Cyber War Will Not Take Place*, 145.
[59] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, 44.
[60] Thomas Rid, *Cyber War Will Not Take Place*, 145.

develop new capabilities to overcome the technical and social levels of the attribution problem if they exercised sovereignty over separate cyberspaces. However, this is not the way the Internet works. The Internet has no national boundaries. This means that, to meet international cyber threats, states with varying interests must voluntarily choose to help one another. But states understand cybersecurity differently. Additionally, if they are not victims themselves, it is questionable to what extent outsiders would invest in helping others attribute an attack.

In the event of a cyber attack, the U.S. military needs to know who is responsible. Yet the technical, social, and political layers of the attribution problem complicate this process. The military does not have the resources to identify its attacker in the event of a serious cyber attack. As a result, it is safer to subordinate cyber power to the other military branches and use cyber weapons only as means of support.

Notwithstanding the arguments presented above, cyber attribution is not impossible. Resolving the technical layer by tracing malicious code to a source is feasible, such as via the use of whois searches. And even if they complicate attribution by launching attacks through a foreign router, hackers and cyber criminals often have a particular style about their attacks. This means that if a series of attacks exhibit similar properties, it might be the case that they were developed and/or launched by the same attacker.[61] Network analysts could then build a profile of this attacker and share their findings with national and international partners.

The technical and social levels of the attribution problem are not impossible. What is most difficult is the political layer. As no country presides over the web, the attribution problem can only be solved via international cooperation. There are currently some promising collaborative initiatives in the making. For instance, the International Cyber Security Protection

[61] Ibid., 160.

Alliance (ICSPA) has recommended that financial institutions collectively shut down virtual currencies, such as Bitcoin, by requiring all monetary transactions to proceed through auditable channels.[62] These measures would help eliminate a conduit for cybercrime that criminals have used to extort payments for kidnapping and contract killing.[63] The public and private sectors would have to work together to succeed, but both have incentives for doing so. Collaboration would protect bank customers, which would enhance states' economic competitiveness and national and cyber security. The web connects public and private entities together. Therefore, to counter threats in cyberspace, it makes sense that these actors must work together.

The issue of attribution in cyberspace is fundamentally a political problem.[64] Cyber attacks occur in a medium that unites the world, so international cooperation might be the best means of making cyber attribution easier. This might explain why some are calling for a 'Correlates of Cyber Warfare" project, which could document information regarding cyber attacks, including time, target IP address, and method of attack, in an effort to facilitate cooperation and information-sharing.[65] Attribution is a problem in cyberspace, but this reflects a lack of interstate cooperation, *not* the intrinsic nature of cyber weapons. As a result, attribution does not convincingly explain why the U.S. has not granted cyber power more operational autonomy.

---

[62] Warwick Ashford, "Time to Review Cyber Trust, Says ICSPA," *Computer Weekly*, published October 23, 2013, accessed February 23, 2013, http://www.computerweekly.com/news/2240207700/Time-to-review-cyber-trust-says-ICSPA.

[63] Warwick Ashford, "McAfee Exposes Scope of Digitally Funded Crime Extends to Contract Killings," *Computer Weekly*, published October 14, 2013, accessed February 23, 2014, http://www.computerweekly.com/news/2240207164/McAfee-exposes-scope-of-digitally-funded-crime-extends-to-contract-killings.

[64] Thomas Rid, *Cyber War Will Not Take Place*, 140.

[65] Charles Debeck, *The Correlates of Cyber Warfare: A Database for the Modern Era* (Ames: Iowa State University, 2011), 14-7.

TECHNOLOGISM REFUTED

Some assert that the U.S. military has not given more operational independence to cyber weapons because of the nature of cyber technology. The argument goes that, as a result of an inability to inflict casualties, determine proportionality, signal one's intentions, or attribute the source of an attack, cyber weapons are too uncertain for further integration. But this is not so. As I demonstrated above, most of these issues are political in nature, oftentimes reflecting a lack of states' willingness to cooperate. Moreover, some of the problems above affect a number of kinetic weapons that play important roles in the American military establishment. Technology therefore fails to explain why cyber weapons are subordinated by the U.S. military.

Strategic Culture

Technologists have failed to explain the current status of cyber power in the U.S. military because they overstate the independent value of technology and undervalue the forces that enable a large organization like the United States military to change. Indeed, Andrew W. Marshall best captured these two observations when he wrote, "the main challenge in…[military change] is an intellectual and not a technological one."[66]

Technology plays a large role in motivating revolutions in military affairs (RMA), changes in activity, effectiveness, and objectives as a result of new technological, systemic, organizational, and/or operational developments.[67] Each RMA is a process by which a military

[66] Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford: Stanford University Press, 2010), 2.
[67] Steven Metz and James Kievit, "Strategy and the Revolution in Military Affairs, from Theory to Policy," *Strategic Studies Institute*, published June 27, 1995, accessed January 20, 2014, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=236.

replaces its core competencies—a nation's central warfighting capabilities—with newer ones.[68] However, as quoted by Dima Adamsky, RMAs involve much more than technology:

> Technology only sets the parameters of the possible and creates the potential for military revolution. What indeed produces an actual innovation is the extent to which militaries recognize and exploit the opportunities inherent in new war, through organizational structures and deployment of force. It was how people responded to technology that produced seismic shifts.[69]

Revolutions in military affairs force militaries to answer two questions: to *what* strategic purposes can new technologies be applied, and *how* can they be applied to best fulfill those purposes.[70] This is no easy task. Military organizations must acknowledge the occurrence or imminence of fundamental change in the social, political, economic, and technological landscapes; from here, they must assemble new tactical, strategic, operational, and organizational structures to accommodate these changes.[71] Such a process involves several steps, including military leaders—with the input of national decision-makers—validating that a revolution is actually in progress, identifying a problem that will be solved by the exploitation of a new technology, and actually exploiting said technology. As a result, revolutions in military affairs occur over years if not decades, with stops and starts separating each stage from another.

Many conceive of the advent of cyber weapons as a revolution in military affairs. This is particularly true with regards to Stuxnet. Paulo Shakarian concludes that Stuxnet has revolutionized war by showing that a piece of software can damage real-world infrastructure.[72] This attack has since raised questions about whether "force" should be redefined under LOAC,

---

[68] Richard O. Hundley, *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?* (Santa Monica: RAND Corporation, 1999), 9.
[69] Dima Adamsky, *The Culture of Military Innovation*, 1.
[70] Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND Corporation, 1997), 117.
[71] Williamson Murray, "Thinking About Revolutions in Military Affairs," *Joint Force Quarterly* (Summer 1997): 73.
[72] Paulo Shakarian, "Stuxnet: Cyber Revolution in Military Affairs," *Small Wars Journal* (April 2011): 8.

as well as how militaries should respond to cyber attacks on national critical infrastructure. Similarly, Tim Hsia and Jared Sperli argue that Stuxnet has altered modern warfare by giving militaries a weapon which allows them to infiltrate enemies' computer networks with or without Internet access, all without jeopardizing their soldiers' lives.[73] In this view, Stuxnet could alter warfare in the long-term by digitalizing the battlefield and making conventional soldiers unnecessary. However, the RMA of cyber power extends even beyond Stuxnet. Lt Col Mark Williamson argues that the very existence of cyber weapons has splintered warfare into three branches: war fought in the physical domains, in the cyber domain, and across both.[74] As such, he concludes the U.S. military needs a new framework of war, such as one mimicking Col John Boyd's Observe-Orient-Decide-Act (OODA) loop in which militaries constantly reorient their worldviews to fulfill their objectives.[75] Colin S. Gray agrees that the advent of internet technology (IT) constitutes an RMA, but he feels that a lack of strategic cyber thought currently limits the applicability of cyber power by the U.S. military.[76]

As explained above, implementing an RMA, including the ongoing revolution in cyber power, is not easy. The U.S. military must venture beyond the existence of new technologies and figure out how to successfully exploit them. To do so, it must analyze its organizational structure, determine and possibly re-sort its priorities, and create new institutions that will make room for its use of new technologies. Much of this process is dependent on the military's norms, rules, behaviors, and historical experience that give rise to its strategic preferences, including in

---

[73] Tim Hsia and Jared Sperli, "How Cyberwarfare and Drones Have Revolutionized Warfare," *At War*, published June 17, 2013, accessed April 20, 2014, http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?_php=true&_type=blogs&_r=0.
[74] Mark L. Williamson, *The Cyber Military Revolution and the Need for a New Framework of War* (Norfolk: Join Forces Staff College, 2012), 42.
[75] Ibid., 66.
[76] Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky is Not Falling," *Strategic Studies Institute*, published April 2013, accessed April 20, 2014, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf.

what ways it is willing to change. These inclinations, which are summed up by the term "strategic culture," affect the U.S. military's conceptualization of when and how to use military force,[77] including how new technologies can be used strategically.

Strategic culture is important because it accounts for the failings of traditional structural theoretical approaches. Neorealism, for example, emphasizes a future-oriented approach in which rational state actors act according to calculations of expected utility. Given their potential advantages, it would be rational for the U.S. armed forces to integrate cyber weapons further. That this has not happened defies rationality. Fortunately, strategic culture accommodates this behavior by acknowledging that strategic actors are socialized differently. Put another way, elites from the United States, Russia, China, and Israel would not make identical strategic choices if put in the exact same situation because they have different backgrounds and experiences informing their decisions. These referent points and ideas constitute strategic culture, which often comes into conflict with rationality.

It is important to note that the U.S. military is not a unitary strategic actor. On the contrary, strategic culture interacts with the U.S. military on three levels: macro-environmental, military organizational, and military sub-organizational. On the first level, the military's strategic choices are shaped by the United States' geography, ethnicity, and history.[78] Other factors include a linear understanding of time, an individualistic national self-conceptualization, and complex power distance dimensions separating the elites from the public.[79]

At this level, the American military has a vision of U.S. culture as a liberal, democratic, Protestant, and capitalistic culture composed of individualistic people who use analytical-logical

[77] Alastair Iain Johnston, "Thinking about Strategic Culture," 46.
[78] Ibid., 37.
[79] Dima Adamsky, *The Culture of Military Innovation*, 16-8.

reasoning to try to make sense of the world objectively, such as by developing new technologies. The military treats the U.S. public as optimistic because it believes their country inspires them to innovate. But the ways in which the American armed services model themselves off this vision are problematic. For instance, they translate perceived American optimism into a military culture of abundance, overwhelming force, and frontal assault with the belief that the United States can subdue all enemies. This philosophy may in some instances prevent the development of more nuanced military strategies. Furthermore, believing the American people are concerned chiefly with the present, the U.S. military resists change and defers to battle-tested tactics which may no longer cohere with the reality of war. This makes it difficult for the services to learn quickly and make changes, including those that relate to new technologies. [80]

The second level on which the U.S. military interacts with strategic culture is the organizational, or military-wide. In this environment, the U.S. military has a vested interest in upholding a strategic culture that extends to every corner of its organizational structure.[81] Towards this end, it has created a series of standard operating procedures (SOPs), regulations outlining how its personnel should respond to a variety of situations.[82] It is expected that each military person will act according to these SOPs.[83] Therefore, to institute change, the U.S. military must reexamine its SOPs that up until now have kept its personnel safe and possibly

[80] Ibid., 75-82.
[81] Colin S Gray, "Strategic Culture as Context: The First Generation of Theory Strikes Back," *Review of International Studies* 25, no. 1 (1999): 63.
[82] Suzanne C. Nielsen, *An Army Transformed: The U.S. Army's Post-Vietnam Recovery and the Dynamics of Change in Military Organizations* (Strategic Studies Institute: Carlisle, 2010), 8.
[83] Jeffrey S Lantis, "Strategic Culture and National Security Policy," *International Studies Review* 4, no. 3 (2002): 91.

institute new ones, which might make its service people feel threatened and resist.[84] Every process of change must navigate these complex organizational dynamics of the military.[85]

It is difficult for the U.S. military to change because, like any large organization, bureaucratic constraints apply. The bureaucratic nature of the services has been well-researched. For example, political economist Max Weber has asserted that the national army represents the ultimate bureaucracy, embodying human civilization's attempt to rationalize everything including war.[86] Additionally, Morton H. Halperin and Priscilla A. Clapp have noted that the American military establishment functions like a bureaucracy in that it uses its influence to mobilize support among members of Congress, veteran groups, and the press for funding.[87]

Like any bureaucracy, the military has its shortcomings. Captain Philip Kreck argues that the military bureaucracy has two problems: fragmentation, where tasks are passed to subordinates without designating recipients; and systems underutilization, where military systems have been complicated by unnecessary procedures.[88] These flaws are responsible for a number of unfortunate incidents. For instance, medevac helicopters in Iraq are required to strictly adhere to the Geneva Convention, which means they must display Red Cross markings on their sides, fly unarmed, and enter into combat zones with armed air support.[89] When there are no escorts, the helicopters cannot fly; when they do, their markings present conspicuous

---

[84] Chad C. Serena, *A Revolution in Military Adaptation: The US Army in the Iraq War* (Washington, DC: Georgetown University Press, 2011), 11.
[85] Williamson Murray, "Innovation: Past and Future," *Joint Force Quarterly* no. 12 (1996): 52.
[86] Robert D. Miewald, "Weberian Bureaucracy and the Military Model," *Public Administration Review* 30, no. 2 (1970): 130.
[87] Morton H. Halperin and Priscilla A. Clapp, *Bureaucratic Politics and Foreign Policy* (Washington, D.C.: Brookings Institution Press, 2006), 238-9.
[88] Captain Philip Kreck, "Fighting the Bureaucracy: Streamlining the 21st-Century Army," *Army Magazine* 57, no. 6 (2007): 13.
[89] James Simpson, "Incomprehensibly Stupid Army Regulation Killing Americans in Afghanistan," *American Thinker*, published January 6, 2012, accessed February 4, 2014, http://www.americanthinker.com/2012/01/incomprehensibly_stupid_army_regulation_killing_americans_in_afghanistan.html.

targets for Al Qa'ida fighters. Instances such as these are the result of strict deference to bureaucratic procedure. The U.S. military therefore functions like a bureaucracy to a fault.

That the U.S. military bureaucracy does not change when perhaps it should is an important point. The military bureaucracy is not only hard to change; it is designed *not* to change.[90] This is because the strategic environment is constantly evolving,[91] and no one can predict when the next war might occur, against whom, under what conditions, and in what arena.[92] Subsequently, in peacetime, with no enemy immediately threatening the United States, the American armed services lack operational tests, i.e. battlefield challenges, to structure their strategic behavior and strategic culture.[93] It would be irresponsible, even dangerous, to re-conceptualize their doctrine in these circumstances, for any change would risk killing American service people by abandoning battle-tested tactics and technology.[94] More than this, in times of peace, the services compete with each other to project their interests onto the next war, which defeats joint research efforts.[95] For these and other reasons, the U.S. military always prepares to fight the *last* war because it has the doctrine and organizational structures to do so.[96] The American armed services innovate only after the realities of war force them to adapt.

The third and final strategic cultural level that relates to the U.S. military is the military sub-organizational, or that which relates to the strategic cultures of individual military branches, such as the U.S. Army or Air Force. While they share the military's cultural mindset overall, the

---

[90] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991), 2.
[91] Suzanne C. Nielsen, *An Army Transformed*, 9.
[92] Williamson Murray, "Innovation: Past and Future," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan R. Millett (Cambridge: Cambridge University Press, 1996), 301.
[93] Suzanne C. Nielsen, *An Army Transformed*, 12.
[94] Ibid.
[95] Major Byron Greenwald, *The Problems of Peacetime Innovation* (Fort Leavenworth: School of Advanced Military Studies, 1995), 23.
[96] Chad C. Serena, *A Revolution in Military Adaptation*, 10.

services cultivate slight differences in thought. In response, unique strategic cultures of trust, loyalty, dedication, *espirit*, and commitment take form.[97]

In the next section, it is on the military organizational level that I explore the current role of cyber power in the U.S. military. I do so by analyzing the evolution of U.S. air power and space power. These two cases share important parallels with cyber power. First, both air power and space power have produced massive technological shifts within the U.S. military. To fully exploit these new conceptualizations of force, the services researched issues such as aerodynamics and jet propulsion, which culminated in the development of strategic bombers and photoreconnaissance satellites. The same can be said with cyber power acknowledging the explosion of ICTs over the past two decades. Second, air power and space power opened up entire new domains to the military. Without air planes and satellites, the American armed services could not have militarized air and space. Similarly, without the advent of computers, a cyber domain would not even exist. Lastly, as with cyber power explained above, many conceive of air power and space power as RMAs. James R. Fitzsimonds and Jan M. Van Tol argue that the development of air power was a revolution in military affairs insofar as the military's integration of airplanes produced a change across all forms of warfare.[98] Meanwhile, Colin S. Gray and James B. Sheldon assert that space power is not only an RMA and a military-technical revolution (MTR); it is also more fundamentally an "evolving physical reality" with which all future wars must contend.[99] In this regard, space power and air power are closely related to cyber power in that all three have created technological booms in the United States,

---

[97] Roger W. Barnett, *Navy Strategic Culture: Why the Navy Thinks Differently* (Annapolis: Naval Institute Press, 2009), 20.
[98] James R. Fizsimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly* (Spring 1994): 25.
[99] Colin S. Gray and John B. Sheldon, "Space Power and the Revolution in Military Affairs," *Airpower Journal* (Fall 1999): 31.

constituted new warfighting domains, and revolutionized military affairs. As a result, the histories of how air power and space power were adopted by the U.S. military are important to understanding U.S. cyber power.

U.S. Air Power and Space Power

The histories of U.S. air power and space power offer insight into American cyber power. The story of air power is one of how war led to military organization change. Prior to the First World War, the U.S. military had no air force to speak of. This led the War Department to view airplanes only as means of support and reconnaissance for the traditional services.[100] The military leadership also wanted to mediate the interservice rivalry of the Army and Navy and allow them to use air power for their separate purposes.[101] As a result, the U.S. military entered into the First World War with airplanes bound to the services. In that conflict, some servicemen began to conceive of air strategy with respect to bombing raids, but the war ended too quickly for U.S. air power to evolve beyond tactical considerations. For the next two decades, some in the military establishment tried to sway public interest towards the development of strategic airpower. Some published books, whereas others conducted air bombing demonstrations off the coast of the Virginia Capes.[102] But the public remained firmly disengaged with war and enjoyed the United States' interwar policy of isolationism. However, the public gradually became interested in air power via airplanes' growing commercial applications in the 1930s, which led the War Department to partially reorganize and give U.S. air forces some operational autonomy.

---

[100] United States, War Dept, Office of the Chief of Staff, *Field service regulations, United States Army, 1914: text corrections to December 20, 1916, changes no. 5* (New York: Army and Navy Journal, 1914), 19.
[101] Martin Caidin, *Air Force: A Pictorial History of American Airpower* (New York: Rinehart & Company, Inc., 1957), 26.
[102] Walter J. Boyne, *The Influence of Air Power upon History* (Gretna: Pelican Publishing Company, 2003), 147.

This became even more pronounced following the bombings of Pearl Harbor. Capitalizing on the public's fear, the War Department created a temporary independent military branch for the air services and, upon the United States' entry into the Second World War, assigned them an important mission: achieve air superiority in Western Europe. At first, the air forces suffered some setbacks. But after they made a few adjustments, the war ultimately swung in their favor. By 1944, the air forces had achieved air superiority, which allowed the Allies to cross the English Channel and win the war. Three years later, the War Department created the United States Air Force, a permanent independent military branch which effectively cemented its recognition of the strategic utility of air power.

The story of space power is one of how the United States restrained the actions of its military. At the end of the Second World War, impressed by the advancements of the Nazis in rocket technology, the United States authorized Operation Paperclip, a covert mission in which the military transported key German rocket scientists, documentation, and equipment to U.S. research facilities.[103] The U.S. military hoped to develop satellites that would enable it to conduct reconnaissance of the Soviet Union.[104] This aspiration deeply interested the services, especially the Air Force, which wanted to lead the charge in missile defense systems.[105] However, the War Department opposed the development of space weapons and instead demanded that the services concentrate on enhancing existing military technology. The interservice rivalry between the services further restrained the development of strategic space power by preventing joint research projects into issues relevant to space exploration. After the

[103] Herbert York, *Race to Oblivion: A Participant's View of the Arms Race* (New York: Simon and Schuster, 1970), 77.
[104] Paul B. Stares, *The Militarization of Space: U.S. Policy, 1945-1984* (Ithaca: Cornell University Press, 1985), 24.
[105] David N. Spires, *Beyond Horizons: A Half Century of Air Force Space Leadership*, ed. George W. Bradley III (Honolulu: University Press of the Pacific, 2002), 10-1.

Soviet Union launched Sputnik, the first manmade satellite, some thought the military would exercise a greater role in space. The public was fearful that the Soviet Union would launch nuclear weapons from space, and the services still wanted funding for research into space weapons. However, following this crisis, the nation's leaders crafted a restrained response. First, they centralized all space programs into a new agency that they hoped would more efficiently mitigate interservice rivalry. Second, acknowledging the United States' growing dependence on satellite technology, they recognized that it was in the country's interest to demonstrate that it could explore space peacefully. They therefore created a separate civilian space agency, which laid the foundations for the U.S. to cooperate with the Soviet Union on a number of anti-weaponization space treaties. These agreements codified norms of peace and cooperation in space, a legacy which has restrained the military's use of space over the past 50 years. Today, the U.S. military still uses space primarily as a means of conducting reconnaissance and as a force enhancer of the traditional armed services.

Given the brief histories above, I observe that four things characterize the development of air and space power: the initial support status of new technologies, the role of popular interest in motivating (or preventing) change, organizational reform following a national crisis, and the centrality of external conflict. In the following pages, I discuss each component in detail. I conclude this section by synthesizing these factors together into a model of military technological integration for the U.S. military.

INITIAL SUPPORT STATUS

The first factor that unites the histories of air and space power is the initial use of new technologies to support the traditional services. With respect to air power, the War Department prior to the First World War asserted: "Military aircraft of all kinds [would] be employed under

the direction of the commander of the forces to which they [were] assigned."[106] Airplanes had never been used in combat, so the War Department concluded they should primarily provide support to the services.[107] Additionally, the U.S. military leadership needed to mediate the rivalry of the U.S. Army and Navy, who were competing for support of their proposed aviation missions.[108] It felt it could best preserve the cohesion of the services by allowing them to use airplanes for their separate purposes. Towards this end, the War Department designated early air power as means of only conducting reconnaissance for the services.[109]

Early space power was similarly constrained by the U.S. military and tied to the services. A chief motivation for the American armed services' decision to militarize space was the desire to launch satellites into orbit and watch the activities of the USSR.[110] If it developed rocketry capabilities before the United States did, it was assumed the Soviet Union would use this technology to terrorize the West and exploit the United States' lack of parallel capabilities.[111] Therefore, the U.S. military felt it needed to develop a photoreconnaissance satellite to prevent this from happening. Some of the services, particularly the Air Force, wanted to go beyond satellite technology and develop long-range missile capabilities. But these ideas did not receive much support from the War Department. Indeed, in 1945, Dr. Vannevar Bush, the newly appointed Chairman to the Joint Research Development Board (JRDB), refused to authorize a joint service research effort into missile technology,[112] instead encouraging the services to focus on improving military weapons that were already in existence.[113] It was more important for the

---

[106] Office of the Chief of Staff, *Field service regulations,* 19.
[107] Ibid.
[108] Martin Caidin, *Air Force*, 26.
[109] Office of the Chief of Staff, *Field service regulations,* 19-20.
[110] Paul B. Stares, *The Militarization of Space*, 24.
[111] James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests* (Stanford: Stanford University Press, 2011), 83.
[112] David N. Spires, *Beyond Horizons*, 38.
[113] Paul B. Stares, *The Militarization of Space*, 24.

military to concentrate on enhancing its existing capabilities—those already employed by the traditional services. However, like air power, this decision was also an attempt to mediate intense interservice rivalry with regards to who would set the agenda for space's militarization. Acknowledging this, Bush confined space R&D to the development of more durable satellites.

PUBLIC INTEREST

A second factor that is evident in an analysis of the histories of U.S. air power and space power is the importance of public interest. During the 1920s and 30s, Americans wanted nothing to do with the military. The First World War still weighed heavily on everyone's minds; the public did not want to think of future wars. As a result, Americans were unmoved by several attempts of U.S. airmen to try to elevate the importance of air power in their minds. These efforts included publishing books on the future of air strategy, as well as conducting bombing demonstrations off the Virginia Capes. Neither succeeded in piquing the public's interest. In fact, it was not until well into the 1930s when non-military applications of aviation technology, including Charles Lindbergh's flights and the advent of commercial airlines, first began to attract people's interest. The War Plans Division of the General Staff took notice and subsequently created the General Headquarters (GHQ) Air Force, a provisional division under which all combat aircraft incorporating new duties such as bombardment were centralized.[114] This was the first major concession the Army and Navy made to strategic air power. Arguably public interest played a major part in motivating their decision to do so.

Public interest played an equally important role in influencing the U.S. military's adoption of space power. From 1970 to 1990, the Soviet Union periodically conducted tests on

[114] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945* (Princeton: Princeton University Press, 2002), 143.

the development of anti-satellite (ASAT) systems. These tests resulted in calls from within the American armed services for more funding with regards to space weapon systems.[115] However, the American people, as well as even some members of the military, did not feel that the Soviet Union was as threatening as it once was.[116] By this point in time, the United States had signed a number of treaties with the Soviet Union prohibiting the weaponization of space. Two in particular deserve mention. The first was the "Outer Space Treaty" (1967), where all signatories agreed to not place installments, colonies, or especially weapons of mass destruction on the Moon, other celestial bodies, or in orbit.[117] The second was the Anti-Ballistic Missile Treaty (1972), under which the United States and the Soviet Union limited their ABM capabilities to just two sites in rejection of nationwide missile defense systems.[118] As a result of increased U.S.-Soviet cooperation, the American people saw no urgency to increase military activity in space. Other events, such as Vietnam, were attracting their attention.[119] The American public therefore resisted calls from within the U.S. military to support further funding for its space programs, which caused the military's space budget to plummet in the 1970s.

These instances illustrate three things. First, the military regards public interest as a significant factor when integrating new technologies into its command structure. It would not have sought public support for airplanes and the possibility of space weapons if it did not think it could help them integrate these technologies. Second, public interest operates independent of the services. In both cases, the U.S. military failed to manipulate the American people into

---

[115] Paul B. Stares, *The Militarization of Space*, 72.
[116] Ibid., 157.
[117] National Aeronautics and Space Administration, History Program Office, *Outer Space Treaty of 1967*, January 1967.
[118] United States, State Department, *Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*, October 1972.
[119] Paul B. Stares, *The Militarization of Space*, 99.

supporting their aims because the public was concerned about other matters, such as avoiding another world war and Vietnam. Lastly, because of an unsupportive public, the U.S. military was unable to overcome the opposition preventing its further integration of new technologies. Without public interest, the American armed services were unable to surmount these challenges.

A NATIONAL CRISIS

Perhaps the U.S. military actively seeks the public's support because it knows how influential it can be in times of a national crisis—the third similarity uniting the air power and space power histories. On December 7, 1941, the Imperial Japanese Army attacked Pearl Harbor, killing 2,400 people and destroying an appreciable number of aircraft and naval vessels. Pearl Harbor was ultimately responsible for the United States' decision to enter into the Second World War. More than that, however, it was the nation's first direct encounter with the destructive effects of strategic air power. The resultant fear and outrage by the American people in no small part motivated President Roosevelt to appoint Henry H. Arnold as Commanding General, Army Air Forces (AAF) in March of 1942.[120] The War Department also reorganized itself over the next few months, during which time it disbanded some of the other scattered air commands, increased the representation of air servicemen, and allowed the AAF to formulate its own strategies.[121] Through this national crisis and its aftermath, the War Department underwent organizational change which ultimately gave the AAF greater operational autonomy.

With respect to space power, the Soviet Union's launch of Sputnik, the world's first ever manmade satellite, also deeply affected the American people. Sputnik was a technological and

---

[120] "General Henry H. Arnold," *U.S. Air Force Biographical Dictionary*, accessed March 24, 2014, http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/107811/general-henry-h-arnold.aspx.
[121] "Chapter II: The Marshall Reorganization," *The United States Army Center of Military History*, accessed March 24, 2014, http://www.history.army.mil/books/root/chapter2.htm.

psychological setback for the United States.[122] Technologically, Sputnik improved the scientific image of the Soviet Union, seeming to affirm its claims that it had superior scientific and military technology.[123] Psychologically, since the Soviet Union had been the first to make tangible headway into space, Americans feared it would now exploit this military advantage by launching nuclear strikes against the United States from space. In response to this fear, President Eisenhower established the Advanced Research Projects Agency (ARPA) and granted it authority over all U.S. space projects.[124] At the same time, the President realized the importance of improving the United States' image of using space for "peaceful" purposes. Subsequently, Eisenhower signed the Space Act in 1958, setting up the National Aeronautics and Space Administration (NASA) as a separate civilian space agency pace. In doing so, he laid the foundations for U.S.-Soviet cooperation on the goal of delegitimizing space's weaponization.

Clearly, Sputnik and Pearl Harbor were different national crises. It is much different to have a military base attacked and thousands of people killed than to have a satellite launched into space. Perhaps this difference helps to explain why officials in the George W. Bush administration invented the term "Space Pearl Harbor" to appeal to people's sense of fear in an attempt to gain support for missile defense research. Nevertheless, they played an important role in the case studies of U.S air and space power. Pearl Harbor and Sputnik elevated the relevance of airplanes and satellites, as well as created a sense of profound fear and vulnerability in the American people. In both instances, the President responded by authorizing at least a partial reorganization of the military, which in turn expanded the functions and strategic importance of

---

[122] James M. Gavin, *War and Peace in the Space Age* (New York: Harper & Brothers, 1958), 14.
[123] Steven Lambakis, *On the Edge of Earth: The Future of American Space Power* (Lexington: The University Press of Kentucky, 2001), 12.
[124] *History of Strategic Air and Ballistic Missile Defense, Volume II: 1956-1972* (Washington, DC: U.S. Army Center of Military History, 2009), 40.

new technologies. Therefore, given possible infighting as well as outlying institutional constraints, a national crisis is sometimes necessary to unite the nation's leaders and services behind the idea of the military further integrating a new technology.

EXTERNAL CONFLICT

Finally, the centrality of external conflict unites the histories of air and space power. Notwithstanding its rejection by the U.S. military, strategic air thought first began to take form over the course of the First World War. A significant contribution to this movement was the advent of trench warfare, which forced the allies to broaden their air tactics to include artillery spotting and bombing raids. Then, some 20 years later, Germany, Japan, and Italy began a massive build-up of their respective national armies, including their aviation capabilities. These developments deeply troubled the United States and convinced President Roosevelt, among others, that strategic air power would serve a crucial function in the next war. As a result, Roosevelt in 1939 signed the National Defense Act, providing the Air Corps with nearly 50,000 new recruits, 6,000 planes, and a $300 million budget to beef up its ranks.[125] Roosevelt also helped create the Army Air Forces (AAF), a temporary yet nonetheless independent branch of the War Department.[126] Following the attacks of Pearl Harbor, General Henry H. Arnold, the Commanding General of the AAF, expanded the nation's air capabilities, building a force of 80,000 aircraft and 2.4 million personnel.[127] This newly formed armada received an important mission: it needed to achieve air superiority in Western Europe to allow for an Allied cross-

[125] Daniel L. Haulman, *One Hundred Years of Flight: USAF Chronology of Significant Air and Space Events 1903-2002* (Maxwell AFB, AL: Air Force History and Museums Program in association with Air University Press, 2003), 35.
[126] "Missions Part Two: Air Power Comes of Age in World War II," *U.S. Air Force*, accessed November 14, 2013, http://www.airforce.com/learn-about/history/part2/.
[127] Ibid.

Channel invasion into France.[128] At first, the USAAF met with mixed success. But with its operational autonomy, the AAF was able to make four adjustments: first, it increased the size of its forces; second, it adopted non-visual bombing techniques to allow for bombing raids in unfavorable European weather; third, it created long-range fighter escorts, which allowed U.S. bombers to penetrate deeper into enemy territory; and lastly, it allowed fighters, instead of merely serving as escorts of American bombers, to engage the enemy.[129] The USAAF analyzed its objectives and independently instituted changes. These adaptations ultimately helped produce the war's turnaround in favor of the Allies. After pounding German defenses, it was clear that by March of 1944, the AAF owned the skies.[130] This American air superiority allowed the Allies to cross the English Channel on June 6, 1944, gain a foothold in Europe, and win the war.

With regards to the U.S. space program, the U.S. military wanted to enhance its space power because it did not want to cede any military advantage to the Soviet Union. This desire became especially pronounced after October 4, 1957 when the Soviet Union successfully launched Sputnik 1 into orbit.[131] Even so, the nation's civilian leaders did not support a larger military presence in space. The U.S. military needed satellites to observe the activities of the USSR. But many policymakers felt it did not need orbital WMDs or satellite bombers. Eisenhower hoped to avoid creating this reality.[132] As a result, he created a special committee to provide some recommendations. The Purcell Panel, as it was called, eventually concluded that the United States' space program needed to differentiate between "exploration" (a civilian

---

[128] Walter J. Boyne, *The Influence of Air Power upon History*, 239.
[129] Kenneth P. Werrell, *Death from the Heavens: A History of Strategic Bombing* (Annapolis: Naval Institute Press, 2009), 114-17.
[130] Ibid., 119.
[131] Natalie Bormann and Michael Sheehan, "Introduction," *Securing Outer Space*, ed. Natalie Bormann and Michael Sheehan (New York: Routledge, 2009), 1.
[132] Michael Krepon and Christopher Clary, *Space Assurance or Space Dominance?: The Cast Against Weaponizing Space* (Washington, DC: The Henry L. Stimson Center, 2003), 30-2.

function) and "control" (a military function).[133] Purcell therefore helped to sponsor the idea of a civilian agency leading peaceful operations in space separate from the military. More significantly, however, the panel outright rejected the development of space weapons as "clumsy and ineffective ways of doing a job," supporting the idea that the Earth was the best domain in which wars could be fought and won.[134] In fact, if the United States were the first one to weaponize space, other states might follow its lead, leading to an arms race.[135] In his view, he saw that it was in the interest of the U.S. military to not weaponize space. These findings of the Purcell Panel have directed the U.S. military's space program ever since, defeating various attempts at space weaponization such as Reagan's Strategic Defense Initiative and George W. Bush's plans for missile defense.

Airplanes and rocket technology arguably existed before the First World War and the Cold War, respectively; if the U.S. military had wanted to use them to develop new weapons, it could have. But it did not. Instead it conceived of air power and space power in response to external threats, particularly as means that would allow it to overcome the challenges of ongoing wars in which it was engaged. The utility of thinking about air power and space power rested on the promise of turning the tide of these wars in the United States' favor.

A MODEL FOR TECHNOLOGICAL INTEGRATION

An analysis of how U.S. air power and space power emerged reveal four commonalities: the initial support status of new technologies, the role of popular interest in motivating (or preventing) change, organizational reform following a national crisis, and the centrality of

---

[133] David S. F. Portree, "NASA's Origins and the Dawn of the Space Age," *National Aeronautics Space Administration History Division*, published February 8, 2005, accessed March 16, 2014, http://www.hq.nasa.gov/office/pao/History/40thann/nasaorigins.htm.
[134] Bob Preston, et al., *Space Weapons, Earth Wars* (Santa Monica: RAND Corporation, 2002), 145.
[135] Michael Krepon and Christopher Clary, *Space Assurance or Space Dominance?*, 76.

external conflict. Together, they create a model that can help us understand the cultural reasons for how the U.S. military chooses to integrate a new technology into its organizational structure and, if so, how far.

U.S. Cyber Power

In this section, in order to examine how the histories of American air power and space power influence our understanding of cyber power, I use my model of technological integration to examine the U.S. military's cyber policy. I observe, among other things, that the current status of cyber power reflects the cases of air and space power. I then conclude by identifying an important trend: as a result of the growing number of apparent applications of cyber weapons, the unlikelihood of a cyber warfare convention, and the proliferation and decreasing costs needed to develop a cyber weapon in today's world, states and non-state actors alike have an increasing incentive to use cyber weapons to attack the United States. Such an attack is the most likely way for U.S. cyber power to change and receive greater operational autonomy.

APPLYING THE CULTURAL MODEL

As explained in the introduction, cyber power is primarily used for support at this time, which fulfills the first criterion of my model. The mission of USCYBERCOM is to protect DoD communication networks and to coordinate the use of cyber weapons with regards to full-spectrum military operations. In this sense, cyber power enhances the traditional services' effectiveness and improves the DoD's overall functionality. Network-centric operations have revolutionized war in that they have made computers integral to the use of military force. To successfully coordinate any use of military force, it is crucial that the military's leaders be able to communicate with one another and with commanders on the battlefield. In seeking to protect

this capability, cyber power enables the strategic coordination of land, air, sea, and space power in war and, by extension, augments the effectiveness of each service's force contribution.

This particular conceptualization of cyber power is also reflected in some of the most recent U.S. cybersecurity documents. For instance, in *The International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, the Obama administration makes the following statement:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[136]

This passage asserts that if actors engage in "hostile acts in cyberspace" against the U.S., the President reserves the right to respond. However, beyond restating the United States' commitment to defend its cyberspace, this document falls short of explaining what "certain hostile acts" would cause the U.S. to contemplate a military response. It neglects to explain what acts, targets, and effects would be necessary to justify force. Moreover, the document fails to articulate an escalation ladder for when the U.S. can use "diplomatic, informational, military, and economic" means in response to cyber attacks. There is no response framework, only the President's affirmation that the U.S. can respond in a variety of ways. This limits the U.S. military's ability to respond to cyber attacks with force. Meanwhile, ordinary cyber operations fall under the mission of USCYBERCOM: they help safeguard DoD networks and communication capabilities, as well as provide support to the traditional services.

---

[136] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (Washington, DC: White House, 2011), 14.

The DoD has also reaffirmed using cyber weapons for communication and support in a report published last year. As a result of the growing cyber threat confronting the country, the report asserts that the United States needs to protect its nuclear deterrent in the face of serious cyber attacks.[137] It makes this point because of survivability: just as traditional nuclear deterrence incorporates this notion, so too should cyber policy in the event of a catastrophic cyber attack.[138] But the DoD is careful to emphasize that the U.S. military will respond to a cyber attack with conventional or nuclear force only if attackers tamper with hardware that systematically corrupts vital governmental networks, or if cyber weapons are part of a larger military operation.[139] Both of these scenarios support the assumption that cyber power is a means of support. The DoD sees that cyber operations must be paired with either economic/industrial exploitation or kinetic force to constitute military action or warrant military reprisals. Cyber attacks do not *by themselves* constitute top-tier threats, a fact which USCYBERCOM's mission reflects. Cyber weapons are strategic only when they support the traditional services.

As in the cases of air power and space power, public interest is another important factor that shapes the U.S. military's interaction with cyber power. According to a 2013 poll conducted by SurveyMonkey in partnership with Bloomberg West, only 21 percent of Americans are concerned most about national cybersecurity; more than half are chiefly worried by the prospect of domestic terrorism, whereas a quarter are focused on either missile defense or the war on

[137] U.S. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013), 42.
[138] Ibid.
[139] Ibid., 23.

drugs.[140] This might help to explain why despite its rhetoric, the U.S. military has not explored the use of cyber weapons in greater depth. Just like war-weariness deterred the development of strategic air power in the 1930s and Vietnam blocked the weaponization of space in the '60s and '70s, other threats are monopolizing most Americans' worries and preventing a deeper integration of U.S. cyber power by the U.S. military.

But the issue goes much deeper than that. Domestic terrorism, missile defense, and the war on drugs all carry their own obstacles, but the American people arguably understand these threats better than cybersecurity. After all, millions of Americans experience the reality of counterterrorism on a daily basis whenever they encounter a Transportation Security Administration (TSA) checkpoint. And while missile defense and the war on drugs might not be as immediate, they conjure up images of familiar concepts, such as satellites conducting reconnaissance of missile sites and law enforcement officials arresting drug traffickers. These threats and their responses, if not already integrated into the backdrop of everyday life, are at least conceivable without requiring too much imaginative power. The American people understand both what is at stake and what can be done.

By contrast, many Americans do not come into contact with cybersecurity on a daily basis and, as a result, do not understand the threat very well. For example, in its 2013 Small Business Technology Survey, the National Small Business Association found that while 94 percent of small businesses are at least somewhat concerned about the prospect of a cyber attack, at least a quarter of owners have little understanding of cybersecurity in general or how to protect

[140] David Goldberg, "How Aware are Americans about Cyber Security?," *SurveyMonkey and Bloomberg West*, published May 2, 2013, accessed March 25, 2014, http://www.slideshare.net/SurveyMonkey/cyber-security-20419475, 17.

their businesses' online security.[141] Similarly, while a number of Americans are concerned about the prospect of cyber attackers shutting down civilian critical infrastructure or infiltrating national defense systems,[142] at least forty percent of Americans have never heard of Stuxnet, let alone have any idea about the types of cybersecurity legislation that Congress is considering.[143] Most Americans are unaware of the major issues that pertain to cybersecurity.

Without a fundamental understanding of cybersecurity, the U.S. public is willing to let others make policy decisions for them without vocalizing what interests they specifically want defended. They understand cyber threats only in the context of the web and therefore feel comfortable entrusting the military with their cybersecurity. In actuality however, the military's activities online account for only a small portion of its cyber activities.[144] In not understanding what is fully meant by the term "cyberspace," the American people are disassociating from the issue of cybersecurity and blindly entrusting others with their interests. This disengagement extends beyond the military, too. A joint poll taken by Associated Press and the GfK Group after the fall 2013 Target breach reveals that an overwhelming majority of Americans feel that it is the responsibility of retailers to guarantee their cybersecurity.[145] They want businesses to do whatever it takes to protect their security online, even at the expense of privacy.[146]

---

[141] "2013 Small Business Technology Survey," *National Small Business Association*, published September 2013, accessed March 25, 2014, http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf, 9.
[142] David Goldberg, "How Aware are Americans about Cyber Security?," 3.
[143] Kayte Korwitts, "Are Americans Concerned About Cyber Security?," *SurveyMonkey*, published May 2, 2013, accessed March 25, 2014, https://www.surveymonkey.com/blog/en/blog/2013/05/02/are-americans-concerned-about-cyber-security/.
[144] Sydney J. Freedberg, Jr., "Cyberwar: What People Keep Missing About The Threat," *Breaking Defense*, published January 6, 2014, accessed March 25, 2014, http://breakingdefense.com/2014/01/cyberwar-what-people-keep-missing-about-the-threat/.
[145] David Bisson, "AP-GfK Poll: Business As Usual For American Consumers After Target Breach," *Information Security Buzz*, published January 28, 2014, accessed March 26, 2014, http://www.informationsecuritybuzz.com/ap-gfk-poll-business-usual-american-consumers-target-breach/.
[146] Tim Wilson, "Survey: U.S. Citizens More Worried About ID Theft Than Privacy," *Dark Reading*, published December 27, 2013, accessed March 26, 2014, http://www.darkreading.com/end-user/survey-us-citizens-more-worried-about-id/240165029?_mc=MP_IW_EDT_STUB.

The instances above suggest that the U.S. public does not feel it needs to engage issues related to cybersecurity. It believes other actors such as the American armed services and private retailers have a greater responsibility to tackle cyber threats, so it feels that these actors can simply act according to its interests. But because it does not fully understand cybersecurity, the U.S. public cannot prescribe what information it wants these actors to protect or how. Subsequently, the military and retailers must speculate what constitutes the public's interest. The U.S. military therefore works to protect the American people from the vantage point of its own organizational strategic culture, or the belief that cyber power should be securitized. The way to go about implementing such an interpretation may not necessarily coincide with the public's interest. But in the absence of an informed opinion with regard to how it wants to be protected in cyberspace, the public cannot say or do much otherwise.

In not wanting to engage the cybersecurity debate, the U.S. public creates a problem for the American military. As I noted earlier, public interest helped the military to overcome obstacles that were blocking the emergence of strategic air and space power. Following Pearl Harbor, the American people's outrage gave rise to the reorganization of the War Department and a reinvigorated AAF. Similarly, the public's fear of nuclear attack after the launch of Sputnik spurred the President to centralize the nation's space program in ARPA. The public's response to national crises—the third component of my model—played an important role in leading the U.S. military to further integrate air and space technologies.

The same cannot be said for cyber power, for there has yet to be a national crisis that unites the American people behind the issue of cybersecurity. That is not to say there has not been talk of such a crisis. In October 2012, then Secretary of Defense Leon Panetta warned about the possibility of a "cyber Pearl Harbor." This attack would be powerful enough to

damage several civilian critical infrastructure at once, degrade military and communication networks, and paralyze the nation with the shock of its physical destruction and abundant loss of life.[147] In order to avoid such a devastating assault on the United States, Panetta and others have been trying to appeal to the public to support the development of new cyber weapons. Once it acquires these new capabilities, the U.S. military could then more actively protect the United States' interests in cyberspace.

While there is some cause to be concerned about an attack on the scale of a "cyber Pearl Harbor," many computer network experts believe that the U.S. military has exaggerated the cyber threat. Renowned American cryptographer and writer Bruce Schneier, for instance, notes that there is indeed a cyber threat confronting the United States, but the words we use to describe it have meaning. If the U.S. public accepts a characterization of the threat as "cyber war," the nation assumes a state of helplessness which demands the military take over for its cybersecurity; however, if the term "cybercrime" is used instead, this makes cybersecurity an everyday function of the judicial system.[148] The term "cyber war" serves the interests of a few, including the military, in that it gives it power and money to broaden its authority.[149] But this influence sends the wrong message and elevates the likelihood of starting a cyber arms race. In Schneier's mind, the United States needs peacetime cybersecurity.[150]

Schneier is not the only observer who has criticized the American armed services for exaggerating the cyber threat. Larry Clinton, President of the Internet Security Alliance, argues

---

[147] U.S. Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, New York City, October 11, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
[148] Bruce Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated," *Schneier on Security*, published July 7, 2010, accessed March 26, 2014, https://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.
[149] Bruce Schneier, "Fear Pays the Bills, but Accounts Must be Settled," *The New York Times*, published June 11, 2013, accessed March 26, 2014, http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/fear-pays-the-bills-but-accounts-must-be-settled.
[150] Bruce Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated."

that the Chinese cyber threat is exaggerated insofar as it is not in the interest of the People's Liberation Army (PLA) to use cyber attacks to destabilize the American economy when China owns so much U.S. debt.[151] Also, given the United States' impressive cyber capabilities relative to those of China, including its vast array of IT applications and R&D, it would appear that cyberspace seems to further demarcate the strong from the weak states.[152] In this view, Clinton concludes that while terrorists and rogue states might want to destabilize the United States, these actors do not have the technological capabilities to do so.[153] This means that the real cyber threat does not arise from malicious actors trying to take down the military but from those who steal national and private intellectual property.[154] Some officials in the DoD have asserted as much: at the 2012 Air Force Association cyber conference, many of the speakers agreed that Cyber Pearl Harbor has already happened.[155] The catastrophe has been threefold: global cybercrime is now more profitable than the drug trade, the U.S. has lost its technological advantage as a result of the proliferation of cyber capabilities, and many American intellectual property rights have been stolen.[156] Given this type of threat, what is needed is more cooperation between the federal government and private industries—*not* a militarized cyber response based on fear.[157]

---

[151] Larry Clinton, "Exaggeration Unfairly Shifts Responsibility," *The New York Times*, published June 10, 2013, accessed March 26, 2014, http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/exaggerating-threats-shifts-responsibility-to-busines.
[152] Lu Jinghua, "China's Cyber Threat: Real or Imaginary?," *China-United States Exchange Foundation*, published June 7, 2013, accessed March 26, 2014, http://www.chinausfocus.com/peace-security/chinas-cyber-threat-real-or-imaginary/.
[153] Larry Clinton, "Exaggeration Unfairly Shifts Responsibility."
[154] Ibid.
[155] Philip Ewing, "Has the 'Cyber Pearl Harbor' Already Happened?," DoD Buzz, published March 26, 2012, accessed March 26, 2014, http://www.dodbuzz.com/2012/03/26/has-the-cyber-pearl-harbor-already-happened/.
[156] Ibid.
[157] Jerry Brito, "Measured Response to a Limited Threat," *The New York Times*, published October 17, 2012, accessed March 26, 2014, http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/let-industry-make-a-measured-response-to-a-limited-cyber-threat.

Clearly, while former Secretary of Defense Panetta and other DoD officials have in the past warned about the threat of a "cyber Pearl Harbor"—and continue to do so[158]—most cybersecurity professionals and computer experts feel that the U.S. military is exaggerating this scenario. This counter-movement based upon a moderate approach to cybersecurity poses a serious challenge to the American armed services in that it openly questions the wisdom of militarizing cyberspace too much. Schneier's concern with the need to avoid a cyber arms race parallels the Purcell Panel's rejection of space weaponization for fear of sparking an arms race in space. And without public support for the development of more sophisticated cyber weapons, the U.S. military currently has little chance of overcoming such an obstacle and justifying a deeper integration of cyber power. What could change this would be an attack on the scale of a Cyber Pearl Harbor. However, officials in the military have been warning about such an event since the 1990s. Such a devastating cyber event may never take place or, if it does, may not do so for years to come. In the meantime, the prospect of the U.S. military using cyber power beyond supporting the services appears bleak.

Finally, like air power and space power, external conflict has proven essential to the evolution of cyber power. It was during the Cold War that scientists first conceived of linking computers together into the Advanced Research Projects Agency Network (ARPANET) as a way of preserving military communication capabilities in the event of a nuclear attack.[159] This was not a response to a Soviet advantage in cyber power relative to the United States. Such an advantage did not exist. Rather, cyber power was meant to protect DoD communication

---

[158] Alastair Stevenson, "US Government Failing to Prepare for Cyber Pearl Harbor, says Ex-Defense Secretary," *V3.co.uk*, published October 4, 2013, accessed March 26, 2014, http://www.v3.co.uk/v3-uk/news/2298636/us-government-failing-to-prepare-for-cyber-pearl-harbor-says-ex-defence-secretary.

[159] "A Brief History of the Internet," *Board of Regents of the University System of Georgia*, accessed March 26, 2014, http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

channels and, in the event of war, the traditional services' ability to respond. Cyber power has therefore always functioned as a means of supporting the services in the context of war.

In addition to helping spark its conceptualization, war has played an important role in shaping cyber power in practice. The U.S. military has used cyber weapons in war since the late-1990s. Its first experiment with cyber power occurred during the Kosovo intervention. In 1998, the United States hacked into the Serbian air defense systems in order to confuse Serbian air traffic controllers.[160] This attack enabled the U.S. military to better protect its bombers, thereby increasing the effectiveness of NATO's air campaign in the region. Even so, the American armed services decided against launching an all-out cyber war against Serbia. It did so for two reasons. First, military planners were concerned that an extended cyber campaign would reveal too much about U.S. cyber capabilities. In their minds, a cyber war would give the Serbian forces, as well as other enemies of the United States, an incentive to develop their own cyber weapons and launch retaliatory strikes. This could permanently erase the U.S. military's cyber advantage.[161] Second, the United States did not want to be convicted of war crimes. Had it used malware to attack a few Serbian banks, the U.S. military could have frozen Serbia leader Slobodan Milosevic's accounts, which may have driven Milosevic to accept defeat. However, the U.S. military refrained because it did not want to cause collateral damage and make thousands of Serbian civilians suffer.[162] The United States wanted to keep the moral high ground, so it rejected cyber war and instead used cyber weapons infrequently to support its air capabilities. Cyber war, in the opinion of the U.S. military, would invite retaliatory strikes and

[160] "History of Known Cyber Attacks," *Cyberwarzone*, published February 7, 2010, accessed March 27, 2014, http://www.cyberwarzone.com/history-known-cyberattacks.
[161] Julian Borger, "Pentagon Kept the Lid on Cyberwar in Kosovo," *The Guardian*, published November 8, 1999, accessed March 27, 2014, http://www.theguardian.com/world/1999/nov/09/balkans.
[162] Ibid.

international condemnation. These costs did not justify any further use of U.S. cyber power in that conflict.

Five years later, the United States invaded Iraq, and once again it drew upon its cyber assets for support. In particular, the Bush administration ordered a cyber attack on mobile phones, computers, and other communication devices used by terrorists to plan roadside bombings.[163] This attack enabled the National Security Agency (NSA) to feed false information to the insurgents, many of whom were led into a trap and subsequently captured or killed.[164] Clearly, the U.S. military valued cyber weapons for their ability to sow disinformation, deceive the enemy, and overall manipulate an adversary's perception of the battlefield. Acknowledging this, it was likely this experience that persuaded the U.S. military today to assign its cyber forces to protect DoD communication networks for fear of falling prey to the same kind of attacks.

However, the American armed services' use of cyber weapons over the course of the Iraq war echoes the Kosovo intervention almost exactly. In the months preceding the invasion, the United States considered launching a cyber attack against Iraq that would freeze billions of dollars of assets, including Iraq President Saddam Hussein's cash flow; however, for fear of causing collateral damage in the form of economic ruin and civilian suffering, the U.S. eventually decided against it.[165] Additionally, the U.S. military was hesitant to develop an official policy on the use of cyber war techniques for fear of encouraging other actors to develop

---

[163] Alejandro Martinez-Cabrera, "U.S. Military Has Employed Cyber-Tactics in Iraq War," *SF Gate*, published November 16, 2009, accessed March 27, 2014, http://blog.sfgate.com/techchron/2009/11/16/u-s-military-has-employed-cyber-tactics-in-iraq-war/.

[164] Shane Harris, "The Cyberwar Plan, Not Just a Defensive Game," *Nextgov*, published November 13, 2009, accessed March 27, 2014, http://www.nextgov.com/cybersecurity/2009/11/the-cyberwar-plan-not-just-a-defensive-game/45303/.

[165] Steven Elliott, "Cyber Warfare and the Conflict in Iraq," *Infosec Island*, published August 20, 2010, accessed March 27, 2014, http://infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html.

similar capabilities, which could then be used against it.[166] As a result, the United States did not exploit cyber assets to their full potential for fear of the incurring undesirable consequences.

Clearly, the U.S. military early on used cyber weapons to confuse its enemies and support the traditional services. But as the examples of Kosovo and Iraq demonstrate, the United States held back because it did not want to cause collateral damage or lose its technological advantage in cyberspace. Any extensive use of these weapons was simply too costly. As a result, U.S. cyber power received little operational autonomy through the 2000s.

An application of my model to U.S. cyber power reveals the following: first, the U.S. military currently uses cyber weapons as means of support; second, the American people are worried about other issues and do not fully understand the cybersecurity problem; third, no destructive "Cyber Pearl Harbor" has occurred yet, and if it has, this means the cyber threat demands something other than a militarized response; and fourth, the U.S. military has restrained its use of cyber weapons in war for fear of causing collateral damage and inviting retaliatory strikes. Together, these factors explain why the U.S. military has refrained from giving cyber power more operational autonomy. It has done so because, from a strategic cultural standpoint, it lacks the support, the impetus, and the necessary historical experience to do so.

THE POTENTIAL FOR CHANGE

Reflecting on the analysis above, the U.S. may want to integrate cyber power further. The United States has always used cyber weapons as means of support in war, creating a conceptualization of cyber power that cannot easily be changed. But this does not mean that change is impossible. Rather it shifts the emphasis away from the internal dynamics of the U.S.

---

[166] Ibid.

military and moves it into the world of external threats. In this final section, I argue that, as a result of states identifying useful applications of cyber weapons, the unlikelihood of a cyber warfare convention, and the decreasing costs of cyber capabilities, actors have more and more incentive to attack the United States using a cyber weapon. This event is the most likely way the U.S. military would integrate cyber power further.

The first reason why actors have a greater incentive to attack the United States in cyberspace is because actors are discovering tempting real-world situations in which they can use cyber weapons. Schneier and computer experts may support the idea of de-emphasizing the military's engagement with cyberspace in an attempt to avoid a cyber arms race. But officials in Washington do not agree. In a meeting this past February, the National Security Council discussed the idea of using cyber attacks against President Bashar al-Assad's command structure in the ongoing Syrian civil war.[167] Such an attack would have its advantages. In a humanitarian crisis, the United States has no incentive to put forces on the ground; a strategic cyber attack against Syria's air strike capabilities, which Assad has used to bomb urban centers over the course of the civil war, could serve a humanitarian purpose and spare U.S. soldiers' lives.[168] Also, as the attack would undermine Syrian military capabilities only, it would have little to no chance of causing collateral damage. Even so, Obama has been hesitant to use cyber weapons in Syria because of the potential long-term consequences. The United States might interpret a cyber attack as de-escalatory, but other actors might see it as a legitimate means of force.[169]

---

[167] "U.S. Planning for Cyber Attacks on Syria," *PressTV*, published February 25, 2014, accessed March 27, 2014, http://www.presstv.ir/detail/2014/02/25/352145/us-planning-for-cyber-attacks-on-syria/.
[168] Michael Wilner, "White House Mulled Waging a Cyber War in Syria," *The Jerusalem Post*, published February 26, 2014, accessed March 27, 2014, http://www.jpost.com/International/White-House-mulled-waging-a-cyber-war-in-Syria-343564.
[169] David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times*, published February 24, 2014, accessed March 27, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0.

Cyber weapons could therefore open up a new kind of warfare and actually increase the frequency of conflict, not to mention lower the costs of committing an act of aggression in the international system. Acknowledging this, the Obama administration, as well as the U.S. military more generally, is still concerned about the prospect of starting a cyber arms race and exposing the United States to retaliatory attacks. Whether the desire to do humanitarian good in Syria justifies taking these risks remains to be seen.

Russia has also discovered real-world applications of cyber weapons. Over the past seven years, Russia has strategically used cyber attacks in three separate instances of what are now widely recognized as "cyber wars." The first occurred in 2007 when an IP address linked to an official working in the Putin administration flooded the websites of the Estonian president, Parliament, and prime minister after the Estonian authorities relocated a statue of a WWII-era Soviet-era soldier.[170] Russia has denied any involvement in the attacks. A year later in Georgia, as part of a military intervention into South Ossetia to protect "Russian compatriots," Russia launched a broad range of cyber attacks, bringing down multiple government and civilian websites for extended periods of time. The interruptions ultimately forced the Georgian government to temporarily relocate President Mikhail Saakashvili's web site to a web hosting service based in Atlanta in an attempt to deter further intrusions.[171] After Russia achieved its objectives, it ceased its cyber attacks and allowed the Georgian websites to come back online. Lastly, Russian IP addresses are linked with massive DDoS attacks that were launched against

[170] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, published May 29, 2007, accessed March 27, 2014, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all.
[171] Ward Carroll, "Cyber War 2.0—Russia v. Georgia," *Defense Tech*, published August 13, 2008, accessed March 27, 2014, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/.

Ukraine this year, disabling the servers of the National Security and Defense Council as well as downing the websites and even mobile devices of hundreds of Ukraine government officials.[172]

States are discovering real-world uses of cyber weapons. Irrespective of whether Obama decides to use cyber weapons against Assad, the Syrian crisis reveals that nations such as the United States are discovering ways in which they can use cyber weapons to their advantage. The fact that they are even theorizing about cyber power means that cyber weapons are considered a viable method of attack by the U.S. military. Furthermore, Russia's "cyber wars" illustrate that in certain situations, states will in fact use these weapons to their advantage. This means that actors will continue to consider the use of or actually deploy cyber weapons in war. Meanwhile, for those states that have not yet considered developing cyber capabilities of their own, they will more than likely at some point encounter an adversary whose cyber forces will motivate them to establish their own cyber commands. States care about cyber power, and all indications suggest that they will do so even more as other states invest in cyber weapons. These observations suggest that the world will see an increase in the number of "cyber states," of which any one could launch a cyber attack against the United States, which would encourage its military to grant cyber power more operational autonomy.

Second, the unlikelihood of a convention on cyber warfare makes it more likely that an actor might use a cyber weapon against the United States. This is because the perceptions of other states reveal that they conceive of cyber power differently than the U.S. military. In today's world, states do not agree on what cybersecurity entails. While the United States and other Western democracies feel that cybersecurity primarily involves protecting computer

[172] Carol Matlack, "Cyberwar in Ukraine Falls Far Short of Russia's Full Powers," *Bloomberg BusinessWeek*, published March 10, 2014, accessed March 27, 2014, http://www.businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers.

networks against theft and data breaches, Russia, China, and other states feel that cybersecurity also involves information security, which in their minds entitles them to manage the content and communication exchanged over social media platforms.[173] Different actors view the issue of cybersecurity differently, and each state has a vested interest in defending its own view of the problem, thereby creating intense disagreement in the international system. Acknowledging this dissension, it is unlikely that states will be able to arrive at some sort of consensus necessary to create a convention on the use of cyber attacks any time soon, a lack of restriction which allows states to use their cyber weapons however they want. Even separate from states' differing evaluations of cybersecurity, the fact that one type of cyber attack can be used against a diverse set of potential targets, including government websites and critical infrastructure, makes the consistent application of a single body of law in this regard all but impossible.[174] There are simply too many variables. As a result, it is unlikely that any international agreements on cyber war will take form in the near future. Subsequently, states and non-state actors will be able to legitimately create cyber weapons that they could then use against the United States, which could create a large enough reaction among the American people and national leadership to justify the U.S. military giving greater operational autonomy to cyber weapons.

The third and final factor that could lead to a notable cyber attack against the United States is the proliferation of technology and the decreasing costs of developing cyber weapons. What is important here is the distinction between weapons on the scale of Stuxnet and those such as DDoS attacks. The former requires extensive financial and programming experience, as well

---

[173] Adam Segal and Matthew C. Waxman, "Why a Cybersecurity Treaty is a Pipe Dream," *Council on Foreign Relations*, published October 27, 2011, accessed March 28, 2014, http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325.

[174] Lawrence L. Muir, Jr., "The Case Against an International Cyber Warfare Convention," *The Wake Forest Law Review*, published December 2011, accessed March 28, 2014, http://wakeforestlawreview.com/the-case-against-an-international-cyber-warfare-convention.

as insiders who have integral knowledge of the target system's configuration.[175] Admittedly, the costs of developing an attack on the level of Stuxnet has decreased in recent years: whereas it once cost around $100 million to develop, today it costs only $10,000.[176] This obviously lowers the entrance cost into the global cyber arena. However, these types of attacks are nonetheless mainly sponsored by only the most sophisticated cyber states in today's international system and, in turn, used against other states.[177]

The same cannot be said for the vast majority of cyber weapons. These assets, such as botnets which actors can use in DDoS attacks, are inexpensive, easier to develop, and multifunctional.[178] The technology needed to create these types of cyber weapons is proliferating, and the costs of development are steadily decreasing. As a result, it is reasonable to expect that the number of actors capable of producing and using cyber weapons will increase exponentially over the next few years. These actors, which will include terrorist organizations, organized cybercrime syndicates, and commercial institutions, will have interests different than those of states. As non-state actors, they might find the costs of launching a cyber attack against a target such as the United States more acceptable than another state might. Furthermore, while a Stuxnet-level attack is devastating, so is an extended cyber campaign using more common cyber weapons. The proliferation of cyber technology and the drop in costs of producing cyber weapons therefore pose a threat to the United States because they empower actors in cyberspace,

---

[175] Paul F. Roberts, "If This Is Cyberwar, Where Are All the Cyberweapons?," *MIT Technology Review*, published January 27, 2014, accessed March 28, 2014, http://www.technologyreview.com/news/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/.
[176] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times*, published February 6, 2014, accessed March 28, 2014, http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.
[177] Ibid.
[178] Daniel Cohen and Aviv Rotbart, "The Use of Code Mutation to Produce Multi-use Cyber Weapons," *The Institute for National Security Studies*, published July 8, 2013, accessed March 28, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=5163.

especially non-state entities, to launch sustained mid-level cyber campaigns against states that could overtime prove devastating. If—or perhaps when—one or more of these actors directs such a campaign against the United States, the damage overtime might be sufficient for the U.S. military to justify granting greater operational autonomy to its cyber forces.

Together, the three factors explained above—the fact that states are discussing the use of cyber weapons and finding real-world applications for them, the improbability of an international convention on cyber warfare being created, and the proliferation and declining costs of cyber technology—suggest that another state or a non-state entity could launch a cyber attack against the United States. If a state launches a moderately sophisticated attack against the United States or if a non-state actor engages in an ongoing cyber campaign against American government agencies or financial institutions, the U.S. could very well interpret the attack as signifying the emergence of a new type of warfare. In this case, the United States would then go on the defensive and likely provide the military with ample resources to make its cyber forces more autonomous. This would initiate the process of the American armed services integrating cyber power further into their collective organizational structure.

The bombings of Pearl Harbor and the subsequent participation of the United States in the Second World War accelerated the U.S. military's integration of aviation technology, allowing air power to evolve into an independent service of its own right. By contrast, in the absence of a "hot war," the military has integrated space power to only a certain extent, and the process has been much slower. As I argue above, a cyber attack against the United States is the most likely way American cyber power would change in a manner that would mimic the emergence of strategic air power. Should such an attack not occur, it is more likely that the

military's adoption of cyber power will be a much slower, more deliberate process that at least partially reflects the development of U.S. space power.

Conclusion

In this article, I have demonstrated how cultural factors inhibit the U.S. military's integration of cyber power beyond assigning them to protect defense networks and support the traditional services. Towards this end, I challenged the conventional wisdom that the associated technology makes cyber weapons non-useful and not even "weapons." I have shown that technology is not non-contextual. History, including the process by which large organizations such as the U.S. military make changes, is significant. With regards to RMAs, a technology must not only exist. The U.S. military must also create procedures, doctrines, and other organizational features that allow it to shape a technology according to its interests.

The case studies of U.S. air power and space power reveal four factors as a way of understanding how the U.S. military integrates new technology. First, technologies are initially tied to the other services. Second, public interest plays an important role in supporting the U.S. military should obstacles arise. Third, a national crisis can and often does lead to military organizational change. And lastly, as a result of these events, the U.S. military underwent some organizational changes which allowed both air power and space power to evolve in the context of external conflict. These four cultural factors played an integral role in shaping the histories of air and space power and help to explain the current status of U.S. cyber power. While the U.S. military might have an incentive to integrate them further, it does not have the public support to do so. The American people are concerned with other issues, such as domestic terrorism. Furthermore, they do not fully understand the cyber problem and are willing to entrust other

actors to make decisions for them, which negates any impact they might have on encouraging the American armed services to grant cyber power greater operational autonomy. At the same time, the U.S. public listens to a few prominent computer experts, who disagree with the U.S. military's warnings that a "Cyber Pearl Harbor" is around the corner. They note that such a crisis has not occurred yet, that the military's efforts could backfire and lead to a cyber arms race, and that a more measured response to cybersecurity, including government-industry partnerships, is preferable at this time. U.S. cyber power has also evolved in the context of war, particularly in Kosovo and Iraq. But in each of these cases, the United States has shown restraint for fear of causing collateral damage and inviting retaliatory strikes. Together, these cultural factors explain why the U.S. military has not further integrated cyber power.

Then again, this might change. External stimuli in the form of a cyber national crisis, not necessarily on the scale of a "Cyber Pearl Harbor," could occur and cause the U.S. military to grant its cyber forces greater operational autonomy. Three trends make this scenario possible: actors such as the United States and Russia are still discussing and discovering real-world applications for the use of cyber weapons, the international system is unlikely to produce a convention on cyber warfare, and cyber technologies are proliferating and decreasing in cost. These three factors increase the likelihood of a cyber attack against the U.S. Regardless of the attacker's motivation, should such an attack occur, the U.S. would likely acknowledge the emergence of a new form of warfare, go on the defensive, and support the U.S. military in integrating cyber power deeper into its organizational structure.

Going forward, the cultural model I proposed in this paper may be able to explain the statuses of other emergent conceptualizations of military force. One of these is robotics power, which includes military drones. Drones are currently used to support the missions of the

traditional services. They have evolved in the context of irregular warfare, but because of the collateral damage they have caused in recent years, the American public is hesitant to support the U.S. military's further integration of the technology. This could change as the phenomenon of modern warfare, marked by the United States' growing aversion to casualties, continues to take form. Together, cyber weapons and robotics promise to satisfy states' desire to avoid putting their soldiers' lives in jeopardy, so it is reasonable to expect that both will be granted more operational autonomy by the U.S. military at some point. Once integrated, both will increasingly reshape war into battles fought by unmanned, autonomous weapons. This will require scholars and policymakers alike to embrace a new notion of what constitutes violence in the future.

Bibliography

"2013 Small Business Technology Survey." *National Small Business Association*. Published September 2013. Accessed March 25, 2014. http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf.

"A Brief History of the Internet." *Board of Regents of the University System of Georgia*. Accessed March 26, 2014. http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford: Stanford University Press, 2010.

Adams, Thomas K. "Future Warfare and the Decline of Human Decisionmaking." *Parameters* 41 (2011): 5-19.

Andress, Jason, and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*. Waltham: Syngress, 2011.

Ashford, Warwick. "McAfee Exposes Scope of Digitally Funded Crime Extends to Contract Killings." *Computer Weekly*. Published October 14, 2013. Accessed February 23, 2014. http://www.computerweekly.com/news/2240207164/McAfee-exposes-scope-of-digitally-funded-crime-extends-to-contract-killings.

—. "Time to Review Cyber Trust, Says ICSPA." *Computer Weekly*. Published October 23, 2013. Accessed February 23, 2014. http://www.computerweekly.com/news/2240207700/Time-to-review-cyber-trust-says-ICSPA.

Barnett, Roger W. *Navy Strategic Culture: Why the Navy Thinks Differently*. Annapolis: Naval Institute Press, 2009.

Becker, Jo, and Scott Shane. "Secret 'Kill List' Proves a Test of Obama's Principles and Will." *The New York Times*. Published May 29, 2012. Accessed February 13, 2014. http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?_r=3&pagewanted=all&.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*. Princeton: Princeton University Press, 2002.

Bisson, David. "AP-GfK Poll: Business As Usual For American Consumers After Target Breach." *Information Security Buzz*. Published January 28, 2014. Accessed March 26, 2014. http://www.informationsecuritybuzz.com/ap-gfk-poll-business-usual-american-consumers-target-breach/.

Borger, Julian. "Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*. Published November 8, 1999. Accessed March 27, 2014. http://www.theguardian.com/world/1999/nov/09/balkans.

Bormann, Natalie, and Michael Sheehan. "Introduction." *Securing Outer Space*, edited by Natalie Bormann and Michael Sheehan. New York: Routledge, 2009.

Boyne, Walter J. *The Influence of Air Power upon History*. Gretna: Pelican Publishing Company, 2003.

Bright, Peter. "Stuxnet apparently as effective as military strike." *Ars Technica.* Published December 16, 2010. Accessed April 25, 2014. http://arstechnica.com/tech-policy/2010/12/stuxnet-apparently-as-effective-as-a-military-strike/.

Brito, Jerry. "Measured Response to a Limited Threat." *The New York Times*. Published October 17, 2012. Accessed March 26, 2014.

http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/let-industry-make-a-measured-response-to-a-limited-cyber-threat.

Builder, Carl H., Steven C. Bankes, and Richard Nordin. *Command Concepts: A Theory Derived From Practice of Command and Control*. Santa Monica: RAND Corporation, 1999.

Caidin, Martin. *Air Force: A Pictorial History of American Airpower*. New York: Rinehart & Company, Inc., 1957.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media, Inc. 2012.

Carroll, Ward. "Cyber War 2.0—Russia v. Georgia." *Defense Tech*. Published August 13, 2008. Accessed March 27, 2014. http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/.

"Chapter II: The Marshall Reorganization." *The United States Army Center of Military History*. Accessed March 24, 2014. http://www.history.army.mil/books/root/chapter2.htm.

Cimbala, Stephen J. "Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble?" *Strategic Studies Quarterly* 5, no. 1 (2011): 117-131.

Clayton, Mark. "How Stuxnet cyber weapon targeted Iran nuclear plant." *Christian Science Monitor*. Published November 16, 2010. Accessed April 25, 2014. http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

—. "Stuxnet malware is 'weapon' out to destroy…Iran's Bushehr nuclear plant?" *Christian Science Monitor*. Published September 21, 2010. Accessed April 25, 2014.

http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Clinton, Larry. "Exaggeration Unfairly Shifts Responsibility." *The New York Times*. Published June 10, 2013. Accessed March 26, 2014. http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/exaggerating-threats-shifts-responsibility-to-busines.

Cohen, Daniel, and Aviv Rotbart. "The Use of Code Mutation to Produce Multi-use Cyber Weapons." *The Institute for National Security Studies*. Published July 8, 2013. Accessed March 28, 2014. http://www.inss.org.il/index.aspx?id=4538&articleid=5163.

Cohen, Tom. "When Can a Government Kill Its Own People?" *CNN Politics*. Published February 11, 2014. Accessed February 13, 2014. http://www.cnn.com/2014/02/10/politics/us-killing-americans/.

Cooper, Jeffrey R. "Another View of the Revolution in Military Affairs." In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 99-140. Santa Monica: RAND Corporation, 1997.

Danilovic, Vesna. *When Stakes Are High: Deterrence and Conflict Among Major Powers*. Ann Arbor: University of Michigan Press, 2002.

Davis, Jacquelyn K., Robert L. Pfaltzgraff, Jr., Charles M. Perry, and James L. Schoff. "Updating U.S. Deterrence Concepts and Operational Planning: Reassuring Allies, Deterring Legacy Threats, and Dissuading Nuclear 'Wannabes.'" *Institute for Foreign Policy Analysis*. Published February, 2009. Accessed February 16, 2014. http://www.ifpa.org/pdf/Updating_US_Deterrence_Concepts.pdf.

Debeck, Charles. *The Correlates of Cyber Warfare: A Database for the Modern Era*. Ames: Iowa State University, 2011.

de Haan, Willem. "Violence as an Essentially Contested Concept." In *Violence in Europe: Historical and Contemporary Perspectives*, edited by Sophie Body-Gendrot and Pieter Spierenburg, 27-40. New York: Springer, 2008.

Elliott, Steven. "Cyber Warfare and the Conflict in Iraq." *Infosec Island*. Published August 20, 2010. Accessed March 27, 2014. http://infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html.

Ewing, Philip. "Has the 'Cyber Pearl Harbor' Already Happened?" *DoD Buzz*. Published March 26, 2012. Accessed March 26, 2014. http://www.dodbuzz.com/2012/03/26/has-the-cyber-pearl-harbor-already-happened/.

Fitzsimonds, James R., and Jan M. Van Tol. "Revolutions in Military Affairs." *Joint Force Quarterly* (Spring 1994): 24-31.

Freedberg, Jr., Sydney J. "Cyberwar: What People Keep Missing About The Threat." *Breaking Defense*. Published January 6, 2014. Accessed March 25, 2014. http://breakingdefense.com/2014/01/cyberwar-what-people-keep-missing-about-the-threat/.

Gavin, James M. *War and Peace in the Space Age*. New York: Harper & Brothers, 1958.

"General Henry H. Anrold." *U.S. Air Force Biographical Dictionary*. Accessed March 24, 2014. http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/107811/general-henry-h-arnold.aspx.

Gilbert, David. "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog." *International Business Times*. Published February 6, 2014. Accessed March 28, 2014. http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

Goldberg, David. "How Aware are Americans about Cyber Security?" *SurveyMonkey and Bloomberg West*. Published May 2, 2013. Accessed March 25, 2014. http://www.slideshare.net/SurveyMonkey/cyber-security-20419475.

Gray, Colin S. "Strategic Culture as Context: The First Generation of Theory Strikes Back." *Review of International Studies* 25, no. 1 (1999): 49-69.

—. "Making Strategic Sense of Cyber Power: Why the Sky is Not Falling." *Strategic Studies Institute*. Published April 2013. Accessed April 20, 2014. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf.

—, and John B. Sheldon. "Space Power and the Revolution in Military Affairs." *Airpower Journal* (Fall 1999): 23-38.

Greenwald, Major Byron. *The Problems of Peacetime Innovation.* Fort Leavenworth: School of Advanced Military Studies, 1995.

Gubrud, Mark. "US Killer Robot Policy: Full Speed Ahead." *Bulletin of the Atomic Scientists.* Published September 20, 2013. Accessed February 19, 2014. http://thebulletin.org/us-killer-robot-policy-full-speed-ahead.

Halperin, Morton H., and Priscilla A. Clapp. *Bureaucratic Politics and Foreign Policy*. Washington, D.C.: Brookings Institution Press, 2006.

Hamber, Brandon. *Transforming Societies After Political Violence: Truth, Reconciliation, and Mental Health*. New York: Springer, 2009.

Harris, Shane. "The Cyberwar Plan, Not Just a Defensive Game." *Nextgov*. Published November 13, 2009. Accessed March 27, 2014. http://www.nextgov.com/cybersecurity/2009/11/the-cyberwar-plan-not-just-a-defensive-game/45303/.

Haulman, Daniel L. *One Hundred Years of Flight: USAF Chronology of Significant Air and Space Events 1903-2002*. Maxwell AFB, AL: Air Force History and Museums Program in association with Air University Press, 2003.

"History of Known Cyber Attacks." *Cyberwarzone*. Published February 7, 2010. Accessed March 27, 2014. http://www.cyberwarzone.com/history-known-cyberattacks.

History of Strategic Air and Ballistic Missile Defense, Volume II: 1956-1972. Washington, DC: U.S. Army Center of Military History, 2009.

Hongju Koh, Harold. "International Law in Cyberspace." *U.S. Department of State*. Published September 19, 2012. Accessed October 19, 2013. http://www.state.gov/s/l/releases/remarks/197924.htm.

Hsia, Tim, and Jared Sperli. "How Cyberwarfare and Drones Have Revolutionized Warfare." *At War*. Published June 17, 2013. Accessed April 20, 2014. http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?_php=true&_type=blogs&_r=0.

Hundley, Richard O. *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?* Santa Monica: RAND Corporation, 1999.

Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science* 2 (1999): 25-48.

"Iran to launch second stage of Bushehr nuclear plant." *PressTV*. Published March 1, 2014. Accessed April 25, 2014. http://www.presstv.com/detail/2014/03/01/352797/iran-to-launch-2nd-stage-of-bushehr-plant/.

Jervis, Robert. "Signaling and Perception: Drawing Inferences and Projecting Images." In *Political Psychology*, edited by Kristen Renwick Monroe, 293-312. Mahwah: Lawrence Erlbaum Associates, Inc., 2002.

Jinghua, Lu. "China's Cyber Threat: Real or Imaginary?" *China-United States Exchange Foundation*. Published June 7, 2013. Accessed March 26, 2014. http://www.chinausfocus.com/peace-security/chinas-cyber-threat-real-or-imaginary/.

Johnston, Alastair Iain. "Thinking about Strategic Culture." *International Security* 19, no. 4 (1995): 32-64.

Korwitts, Kayte. "Are Americans Concerned About Cyber Security?" *SurveyMonkey*. Published May 2, 2013. Accessed March 25, 2014. https://www.surveymonkey.com/blog/en/blog/2013/05/02/are-americans-concerned-about-cyber-security/.

Kostopoulos, George. *Cyberspace and Cybersecurity*. Boca Raton: Taylor & Francis Group, LLC, 2013.

Kreck, Captain Philip. "Fighting the Bureaucracy: Streamlining the 21st-Century Army." *Army Magazine* 57, no. 6 (2007): 12-4.

Krepon, Michael, and Christopher Clary. *Space Assurance or Space Dominance?: The Cast Against Weaponizing Space*. Washington, DC: The Henry L. Stimson Center, 2003.

Lambakis, Steven. *On the Edge of Earth: The Future of American Space Power*. Lexington: The University Press of Kentucky, 2001.

Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *The New York Times*. Published May 29, 2007. Accessed March 27, 2014. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all.

Lantis, Jeffrey S. "Strategic Culture and National Security Policy." *International Studies Review* 4, no. 3 (2002): 87-113.

Levy, Yagil. "The Tradeoff between Force and Casualties: Israel's Wars in Gaza, 1987-2009." *Conflict Management and Peace Science* 27, no. 4 (2010): 386-405.

Libicki, Martin C. *Crisis and Escalation in Cyberspace*. Santa Monica: RAND Corporation, 2012.

—. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Mars, Perry. "The Nature of Political Violence." *Social and Economic Studies* 24, no. 2 (1975): 221-238.

Martinez-Cabrera, Alejandro. "U.S. Military Has Employed Cyber-Tactics in Iraq War." *SF Gate*. Published November 16, 2009. Accessed March 27, 2014. http://blog.sfgate.com/techchron/2009/11/16/u-s-military-has-employed-cyber-tactics-in-iraq-war/.

Matlack, Carol. "Cyberwar in Ukraine Falls Far Short of Russia's Full Powers." *Bloomberg BusinessWeek*. Published March 10, 2014. Accessed March 27, 2014. http://www.businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers.

Metz, Steven, and James Kievit. "Strategy and the Revolution in Military Affairs, from Theory to Policy." *Strategic Studies Institute*. Published June 27, 1995. Accessed January 20, 2014. http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=236.

Miewald, Robert D. "Weberian Bureaucracy and the Military Model." *Public Administration Review* 30, no. 2 (1970): 129-133.

"Missions Part Two: Air Power Comes of Age in World War II." *U.S. Air Force*. Accessed November 14, 2013. http://www.airforce.com/learn-about/history/part2/.

Moltz, James Clay. *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*. Stanford: Stanford University Press, 2011.

Muir, Jr., Lawrence L. "The Case Against an International Cyber Warfare Convention." *The Wake Forest Law Review*. Published December 2011. Accessed March 28, 2014. http://wakeforestlawreview.com/the-case-against-an-international-cyber-warfare-convention.

Murray, Williamson. "Innovation: Past and Future." *Joint Force Quarterly* no. 12 (1996): 51-60.

—. "Innovation: Past and Future." In *Military Innovation in the Interwar Period*, edited by Williamson Murray and Allan R. Millett, 300-328. Cambridge: Cambridge University Press, 1996.

—. "Thinking About Revolutions in Military Affairs." *Joint Force Quarterly* (Summer 1997): 69-76.

National Aeronautics and Space Administration. History Program Office. *Outer Space Treaty of 1967*. January 1967.

National Security Research, Inc. *Department of Defense Non-Lethal Weapons and Equipment Review: A Research Guide for Civil Law Enforcement and Corrections*, no. 200516. Published June 19, 2003. Accessed February 20, 2014. https://www.ncjrs.gov/pdffiles1/nij/grants/200516.pdf.

Nielsen, Suzanne C. *An Army Transformed: The U.S. Army's Post-Vietnam Recovery and the Dynamics of Change in Military Organizations.* Carlisle: Strategic Studies Institute, 2010.

Osakwe, Chukwuma. "Non-Lethal Weapons and Force-Casualty Aversion in 21st Century Warfare." *Journal of Military and Strategic Studies* 15, no. 1 (2013): 1-20.

Osawa, Jun. "Is Cyber War Around the Corner? Collective Cyber Defense in the Near Future." *Brookings*. Published November 2013. Accessed February 18, 2014. http://www.brookings.edu/research/opinions/2013/11/12-cyber-defense-us-japan-alliance-osawa.

Pantucci, Raffaello. "Cyber War Will Not Take Place." *Rusi Journal* 158, no. 6 (2013): 106-7.

Portree, David S. F. "NASA's Origins and the Dawn of the Space Age." *National Aeronautics Space Administration History Division.* Published February 8, 2005. Accessed March 16, 2014. http://www.hq.nasa.gov/office/pao/History/40thann/nasaorigins.htm.

Preston, Bob, Dara A. Johnson, Sean J. A. Edwards, Michael Miller, and Calvin Shipbaugh. *Space Weapons, Earth Wars*. Santa Monica: RAND Corporation, 2002.

Ray, Larry. *Violence and Society*. New York: SAGE Publications Ltd., 2011.

Rice, Mason, Jonathan Butts, and Sujeet Shenoi. "A Signaling Framework to Deter Aggression in Cyberspace." *International Journal of Critical Infrastructure* 4 (2011): 57-65.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.

Roberts, Paul F. "If This Is Cyberwar, Where Are All the Cyberweapons?" *MIT Technology Review*. Published January 27, 2014. Accessed March 28, 2014. http://www.technologyreview.com/news/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/.

Rosen, Stephen Peter. *Winning the Next War: Innovation and the Modern Military*. Ithaca: Cornell University Press, 1991.

Sanger, David E. "Syria War Stirs New U.S. Debate on Cyberattacks." *The New York Times*. Published February 24, 2014. Accessed March 27, 2014. http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0.

Schelling, Thomas C. "The Strategy of Conflict: Prospectus for a Reorientation of Game Theory." *The Journal of Conflict Resolution* 2, no. 3 (1958): 203-246.

Schneier, Bruce. "Fear Pays the Bills, but Accounts Must be Settled." *The New York Times*. Published June 11, 2013. Accessed March 26, 2014. http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/fear-pays-the-bills-but-accounts-must-be-settled.

—. "The Threat of Cyberwar Has Been Grossly Exaggerated." *Schneier on Security*. Published July 7, 2010. Accessed March 26, 2014. https://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.

Scott, Richard L. *Conflict Without Casualties: Non-Lethal Weapons in Irregular Warfare*. Monterey: Naval Postgraduate School, 2007.

Segal, Adam, and Matthew C. Waxman. "Why a Cybersecurity Treaty is a Pipe Dream." *Council on Foreign Relations*. Published October 27, 2011. Accessed March 28, 2014. http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325.

Serena, Chad C. *A Revolution in Military Adaptation: The US Army in the Iraq War*. Washington, DC: Georgetown University Press, 2011.

Shakarian, Paulo. "Stuxnet: Cyber Revolution in Military Affairs." *Small Wars Journal* (April 2011): 1-10.

Simpson, James. "Incomprehensibly Stupid Army Regulation Killing Americans in Afghanistan." *American Thinker*. Published January 6, 2012. Accessed February 4, 2014. http://www.americanthinker.com/2012/01/incomprehensibly_stupid_army_regulation_killing_americans_in_afghanistan.html.

Spires, David N. *Beyond Horizons: A Half Century of Air Force Space Leadership*, edited by George W. Bradley III. Honolulu: University Press of the Pacific, 2002.

Sprenger, Sebastian. "Air Force General Emphasizes Focus on Nonkinetic Warfare." *Federal Computer Week*. Published September 6, 2007. Accessed February 20, 2014. http://fcw.com/articles/2007/09/06/air-force-general-emphasizes-focus-on-nonkinetic-warfare.aspx.

Stares, Paul B. *The Militarization of Space: U.S. Policy, 1945-1984*. Ithaca: Cornell University Press, 1985.

Stevenson, Alastair. "US Government Failing to Prepare for Cyber Pearl Harbor, says Ex-Defense Secretary." *V3.co.uk*. Published October 4, 2013. Accessed March 26, 2014. http://www.v3.co.uk/v3-uk/news/2298636/us-government-failing-to-prepare-for-cyber-pearl-harbor-says-ex-defence-secretary.

Turner, Michael. "Is There Such a Thing as a Violent Act in Cyberspace?" *International Security and Intelligence Summer School 2013, Pembroke College, and the University of Cambridge*. Accessed February 18, 2014. http://www.pem.cam.ac.uk/wp-content/uploads/2013/04/Is-there-such-a-thing-as-violence-in-cyberspace.pdf.

"U.N. Rights Chief "Seriously Concerned" Over U.S. Drone Strikes in Pakistan, Echoed by Iran." *UN Watch*. Published June 19, 2012. Accessed February 13, 2014. http://blog.unwatch.org/index.php/2012/06/19/u-n-rights-chief-seriously-concerned-over-u-s-drone-strikes-in-pakistan-echoed-by-iran/.

United States. State Department. *Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*. October 1972.

United States. War Department. Office of the Chief of Staff. *Field service regulations, United States Army, 1914: text corrections to December 20, 1916, changes no. 5*. New York: Army and Navy Journal, 1914.

"US Cyber Command." *U.S. Army Cyber Command*. Accessed November 26, 2013. http://www.arcyber.army.mil/org-uscc.html.

U.S. Department of Defense. *Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates.* Published July 29, 2011. Accessed November 26, 2013. http://www.gao.gov/assets/100/97674.pdf.

—. Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. January 2013.

—. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City*. October 11, 2012. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

"U.S. Planning for Cyber Attacks on Syria." *PressTV*. Published February 25, 2014. Accessed March 27, 2014. http://www.presstv.ir/detail/2014/02/25/352145/us-planning-for-cyber-attacks-on-syria/.

"Violence." *Oxford Dictionary*. Accessed February 18, 2014. http://www.oxforddictionaries.com/us/definition/american_english/violence.

Walker, Paul A. "Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine." *National Security Law Brief* 1, no. 1 (2011): 33-67.

Wallace, Jonathan. "Proportionality and Responsibility." *The Ethical Spectacle*. Published August 2006. Accessed February 13, 2014. http://www.spectacle.org/0806/proportionality.html.

Werrell, Kenneth P. *Death from the Heavens: A History of Strategic Bombing*. Annapolis: Naval Institute Press, 2009.

White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: White House, 2011.

Williamson, Mark L. *The Cyber Military Revolution and the Need for a New Framework of War*. Norfolk: Join Forces Staff College, 2012.

Wilner, Michael. "White House Mulled Waging a Cyber War in Syria." *The Jerusalem Post*. Published February 26, 2014. Accessed March 27, 2014. http://www.jpost.com/International/White-House-mulled-waging-a-cyber-war-in-Syria-343564.

Wilson, Clay. "Network Centric Operations: Background and Oversight Issues for Congress." *Congressional Research Service*. Published March 15, 2007. Accessed March 2, 2014. http://www.fas.org/sgp/crs/natsec/RL32411.pdf.

Wilson, Tim. "Survey: U.S. Citizens More Worried About ID Theft Than Privacy." *Dark Reading*. Published December 27, 2013. Accessed March 26, 2014. http://www.darkreading.com/end-user/survey-us-citizens-more-worried-about-id/240165029?_mc=MP_IW_EDT_STUB.

York, Herbert. *Race to Oblivion: A Participant's View of the Arms Race*. New York: Simon and Schuster, 1970.