AU/ACSC/CUMMINS, S/AY15

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE GARRISON DOMAIN:

CIVIL-MILITARY RELATIONS IN THE CYBERSPACE DOMAIN

by

Shannon C. Cummins, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Dr. Ron Dains

Maxwell Air Force Base, Alabama

April 2015

DISCLAIMER

ABSTRACT

This paper will lay out the construct of a garrison domain and what it might look like based on Harold Lasswell's theory of a garrison state. The concepts of the garrison state combined with the differences of the newly formed cyberspace domain highlight causes for concern when evaluating US actions with regards to cyberspace. Additionally, it will explore America's dependence on cyberspace, the threat posed by that dependence, and current actions and policies in cyberspace in order to determine if the United States is on a path to creating a garrison domain.

Cyberspace is everywhere, not physically, but instead in the connections it creates between the people interacting through the domain. Its ability to create virtual connections between people and devices, and cause wide spread strategic effects raises the question: Can the unique and ubiquitous nature of cyberspace support the creation of a garrison domain, and when combined with a critical dependence on this domain, drive the creation of an actual garrison state?

Lasswell's three traits of a garrison state: a persistent, democratized threat; the rise of the specialists in violence; and the focus on research, development, and production on capabilities for war, do not translate directly to a domain like cyberspace.

First, the physical domains are always present whereas the cyberspace domain is not always present, a person can remove themselves completely from the domain. Second, in the physical world the military are the specialists of violence, but in the domain of cyberspace actions are directed at the information within the systems, not at the humans utilizing the domain. Finally, production focused on warfare in the physical world is aimed at producing violence, in cyberspace production is aimed at violence towards the information that fills the domain. The garrison state construct does not work in evaluating the cyberspace domain; instead a new theoretical construct is needed to do this.

The key motivator within a garrison domain is the existence of a democratized threat to society. All other actions are justified based on the existence and acceptance of this threat to society. Once the threat is accepted as real, the relative amount of power, authority, and influence will begin to centralize in the executive branch and military. In evaluating the current political, social, and security environment in the US this paper will determine if a democratized threat exists in cyber and if the power, authority, and influence with regards to the cyberspace domain have become centralized within the executive branch and DOD.

CONTENTS

Introduction

"We the People of the United States, in Order to form a more perfect Union, establish Justice, ensure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."
— Preamble to the Constitution

The words written by the founding fathers above have molded and guided our country for over 200 years. We, the United States, are entering a time in history where dependence on technology is raising concerns about the balance of security and blessings of liberty set forth in our Constitution. Are we, in the name of security, stripping away civil liberties, militarizing our networks, and in turn altering the character of the United States set forth by the Constitution?

Harold Lasswell defined his construct of a garrison state as "a world in which the specialists on violence are the most powerful group in society… away from the dominance of the specialist on bargaining, who is the businessman, and toward the supremacy of the soldier."[1] His article entitled "The Garrison State," sought to conceptualize militarized states like Germany, Japan, and Soviet Russia at a time when these states were rapidly rising in power and causing leaders to rethink the global future based on the Westphalia model.

With the increased use of cyberspace in every aspect of modern life it is time to revisit Lasswell's theory of the garrison state as it might apply to the new domain of cyberspace. This paper will lay out the construct of a garrison domain and what it might look like based on Lasswell's theory of a garrison

state. Additionally, it will explore America's dependence on cyberspace, the threat posed by that dependence, and current actions and policies in cyberspace to determine if the United States is on a path to creating a garrison domain. Finally, this paper will evaluate if a garrison domain could fuel the creation of an actual garrison state.

The Garrison State

Harold Lasswell defined the garrison state as "a world in which the specialists on violence are the most *powerful* group in society."[2] For the purposes of this paper the term 'powerful' encompasses power, authority, and influence. Power is defined as the actual ability to get people to do what you want through the use of force or threat. Authority is defined as the recognized right to make people do what you want. Finally, influence is defined as the ability to get people to do what you want by convincing them it is in their best interests.[3] Lasswell built his construct on three pillars.

First, a threat to the state will be ever-present and democratized, or equal, for all citizens. The introduction of air power in the early 20th Century erased the distinction between combatants and non-combatants, no longer were citizens safe from combat. The bombing of cities in WWII presented an equal threat to every individual of the state, and states with an ever-present and democratized threat of war, or conflict, were more inclined to become garrison states.[4]

Second, a long-term, constant threat would provide a rise to power of the military elite, and freedoms in a society would be reduced as focus on preparation for war became the dominant concern.[5] The constant threat would drive a general trend in which the specialists on violence become the most powerful group, maintaining the highest levels of power, authority, and influence within society.

Finally, the elites would attempt to hold in check the utilization of productive potentialities of modern science and technology. Instead, scare tactics would be utilized to focus production capabilities on means of violence and away from production for non-military consumption.[6] These pillars were brought into existence and strengthened by a driving force, technology.

Lasswell's construct of the garrison state was based on multiple observations, primarily the transformational power of technology, and more specifically, the introduction of airpower and the resulting democratization of threat to governments, militaries, and societies alike. Today's parallel to air power is cyber power and the cyber domain.

The Cyber Domain

The cyber domain came into existence in 1969 through the creation of the Advanced Research Projects Agency Network (ARPANET), and was not codified as a domain until the early part of the 21st century. Born out of military research and design, the domain of cyberspace, unlike the physical domains of land, sea, air, and space, is wholly man-made, existing both in

physical state and logical state. This new domain does not behave as the others do, actions within cyberspace are not limited by physics, time, and space, making it difficult for politicians, militaries, and society to firmly define it. The Department of Defense (DOD) defines cyberspace as;

> "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7]

However, this definition falls short of encompassing the true extent of the cyberspace domain.

We have thus far attempted to define cyberspace as a collection of physical things, of wires, routers, switches, and processors, yet cyberspace is more than that. Cyberspace is everywhere, not physically, but instead in the connections it creates between the people interacting through the domain. Its ability to create virtual connections between people and devices, and cause wide spread strategic effects raises the question: Can the unique, ubiquitous nature of cyberspace support the creation of a garrison domain, and when combined with a critical dependence on this domain, drive the creation of an actual garrison state?

The Garrison Domain

> *"Of all the enemies to public liberty war is, perhaps, the most to be dreaded…War is the parent of armies; from these proceed debts and taxes; and armies, and debts, and taxes are the known instruments for bringing the many under the domination of the few. In war, too, the discretionary power of the Executive is extended…and all the means of seducing the minds, are added to those of subduing the force, of the people."*[8]
>
> – *James Madison*

Lasswell's garrison state construct provides a tool to evaluate if civil-military relations have slewed too far towards military dominance. However, the three traits of a garrison state: a persistent, democratized threat; the rise of the specialists in violence; and the focus on research, development, and production capabilities for war, do not translate directly to a domain like cyberspace.

<u>The Democratization of Threat in Cyber</u>

The cyber domain permeates almost all aspects of modern life. It is drifting slowly away from a focus on its technical makeup towards a societal focus. Government entities depend on it to manage the country, states, cities, towns, and departments. Militaries rely on cyber for command, control, communications, computers, information, surveillance, and reconnaissance. Members of society rely on it to facilitate governance, commerce, communications, and entertainment. The reliance on cyberspace is so predominant it seems unacceptable to not be part of the domain. The domain

is no longer an enabler, or force multiplier, it is an integrator; enablers are nice to have, but integrators are required.

In the past, technological revolutions of airpower and nuclear weapons created a democratized threat to enemies of states equipped with that technology. However, these technologies remain prohibitively expensive, obtainable only by wealthy, advanced states. In contrast, the domain of cyberspace is low-cost and available to all, and because cyberspace exists at all levels of modern society everyone is potentially exposed to the same threats. Harvard lecturer and digital strategist Nicco Mele writes, "Today, national security is fragile, with power shifting to technologically-equipped terrorist groups, revolutionary movements, criminal enterprises, murky collectives such as Anonymous, and even isolated individuals with an Internet connection."[9] The low-cost of entry into the cyberspace domain allows myriad groups and individuals to compromise civilian accounts, industrial systems, and government systems among others.

The democratized threat for a domain is not the same as a democratized threat to a state. Key to a democratized threat is its perceived existential nature. A threat may be universal to all, but without being existential it will not drive the creation of a garrison state. In a garrison domain a societal requirement, or dependence, for all members of the state to be participants must exist in order for the threat to be existential. Within a garrison domain, the refusal of participation would stigmatize a person, making them an outcast,

unable to participate fully in the functions of society, and running the risk of being removed from the domain, and in turn society.

In the theoretical construct of a garrison domain it would be compulsory for society not only to focus on security and warfare, but also to ensure their individual security bolsters the collective security of the domain. To this end, the state would mandate certain standards of operation for continued acceptance within the domain. These mandates would most likely begin at the state level and slowly propagate to the rest of the domain until directed at each individual. It may become infeasible for individuals to maintain the technical skills required to continually satisfy these mandates leading actions to be centralized, automated, and controlled at higher levels by ever smaller and less representative groups of specialists in order to maintain compliance.[10]

Within a state the practices of democracy may be fully functioning, while within a garrison domain these practices would be rendered symbolic or abolished completely. Any remaining semblance of representation would be groups specific to the domain, existing only to ratify standards and policies set forth by the elite, but with almost no authority to direct or overrule centralized decisions. As democracy is abolished within the domain, authority and control become highly centralized among specialists and further supported through the use of classification and secrecy.

Rise of the Cyber Soldier

Within cyberspace the transition of power, authority, and influence to specialists may not be as overt as in the physical realms. The difficulty with the garrison state's specialist on violence is the fact violence cannot exist or emanate from the cyberspace domain. Violence centers on the human body, it originates from the human body, and is meant to directly affect the human body by delivering a significant emotional impact to terrorize, or mentally traumatize the intended target.[11] Actions within cyberspace are directed at information within systems, not at the humans utilizing the domain, and lack the ability to directly deliver terror and violence on their own; they are inherently indirect. Because of these limitations of cyberspace the soldier's expertise would not be on physical violence, but instead on the management and exploitation of the domain's core—information.

It would be expected for many of these specialists on information to come from the world of intelligence; these are the masters of identifying, gathering, and manipulating information. Lasswell also included the policeman in his definition of a specialist on violence, they too rely heavily on gathering, interpreting, and manipulating information to ensure the rule of law remains supreme.[12] Not only would these specialists be experts in the management and manipulation of information, they would also be proficient in skills associated with large enterprise and civilian personnel management.

The transition to specialists on information being the most powerful group in society would be driven by the existence of a long-term, constant

threat to systems of the cyberspace domain. While not seen as an existential threat as is nuclear war, it would be seen as an existential threat to systems upon which modern society currently relies. A persistent threat to the information would bring the supremacy of specialists on information to the forefront as focus on security, and preparation for attacks, becomes the dominant concern.

Focus of Cyber Technology Production Towards War

In a garrison state preparation for war consumes a society completely, leaving little else for non-military purposes or advancement. All social actions are viewed through the lens of state security, including the nation's industrial base. Efforts focus on production of resources and capabilities specialized to acts of violence. The ruling elites in a garrison state utilize scare tactics to maintain a willingness to continue production towards war and away from non-military goods. This focus would carry over to research and development, highlighting the increased technical capabilities and potential for modern civilization based on the framework of the garrison state.[13]

For a garrison domain, preparation for war is more focused on actions and capabilities specifically within the domain. The militarization of the domain may be less visible as compared to militarization of state government. Production within a garrison domain controlled by specialists on information would focus on capabilities to generate, secure, manipulate, and disseminate information as elites within the domain see fit. The functionality and capability

of such products would seem irrelevant to society and would mostly be ignored and the increased utilization of civilian management skills would mask the militarization as the domain begins to look less like a battlefield and more like a civilian enterprise.

In order to maintain relevance and focus, a continuous stream of information supporting the threat would need to be created or gathered, and disseminated. The validity and authenticity of this threat may vary, but through centralization and secrecy this would be difficult if not impossible for society to determine. Additionally, research and design within the domain would be directed towards specialization on information, and would continue to advance exploitation capabilities of technology.

Evaluation of Current Environment

The key motivator within a garrison domain is the existence of a democratized threat to society. All other actions are justified based on the existence and acceptance of this threat to society. Once the threat is accepted as real, the relative amount of power, authority, and influence begin to centralize in the executive branch and military. By evaluating the current environment in the US this paper will determine if a democratized threat exists in cyber and if the power, authority, and influence, with regards to the cyberspace domain, have become centralized within the executive branch and DOD.

Democratization of the Cyberspace Threat

After the fall of the Soviet Union and end of the Cold War the US was left as the sole military superpower, leaving competitors searching for ways to compete. Adversaries turned to asymmetric strategies and methods, and cyberspace became the most asymmetric way to attack the US. This new asymmetric method is having a profound effect on the US and its focus within the cyberspace domain.

The DOD is extremely vulnerable to attacks in cyberspace due to over dependency on information technology and networks. The DOD cyberspace footprint provides for 8.9 million personnel in 146 countries at 5,000 locations with 1,700 data centers, 65,000 servers, and 7 million devices; 20 percent of these are mission critical to national security.[14] The US defense establishment relies on the cyberspace domain and information within to integrate operations to ensure national security.[15]

The threat to US national security in cyberspace goes beyond the military to vulnerabilities in civilian critical infrastructure. In 2007 the Department of Energy conducted a top-secret test to successfully destroy a generator using a cyber attack, and in 2011 demonstrated an attack against a chemical plant. The exercise illustrated the inability of even top experts to defend against an attack from determined hackers. After the tests the Department of Homeland Security (DHS) released a report showing a 52 percent increase in attacks on infrastructure.[16] General Martin Dempsey points out that US military and critical infrastructure both depend on commercial networks. Regardless of how

secure military and infrastructure networks might be they are still only as secure as the weakest civilian network.[17]

In a garrison domain, to be a part of society you must be part of the domain. Participation by society within cyberspace is through the collection, processing, and storage of personally identifiable information (PII). In 2012 there were 93 million identities stolen during cyber-attacks, in 2013 there were 552 million; an increase of 593 percent in one year.[18] As people continue to connect to cyberspace in more diverse ways there will be an exponential increase in the amount of PII available to attackers, only serving to increase the risk and threat to society.

The first trait of a garrison domain not only requires a threat, but a threat that is democratized. Almost every type of person and organization on this planet arguably touches the cyberspace domain, directly or indirectly. Because this domain is required at all levels it exposes all to the same threat. The directed and sometimes state sponsored attacks on information at all three levels; military, government, and civilian, creates a perceived threat to a modern society whose existence is dependent on the cyberspace domain.

Rise of the Specialist on Information

Within a garrison state there is a centralization of power, a transition from the many to the few. So too, within a garrison domain the power is centralized into the hands of a few. This transfer of power, authority, and

influence is from the legislative and society to the executive and military, more specifically, intelligence and law enforcement agencies.

Power is defined as the ability to get people to do what you want through the use of force or threat. The standup of US Cyber Command (USCYBERCOM) in 2010 started with 1,100 personnel, mostly military.[19] Its mission is to direct the operations of specified DOD information networks and when directed conduct full spectrum military cyberspace operations. USCYBERCOM, paired with the National Security Agency (NSA), the preeminent signals intelligence agency, has slowly expanded its ability to cause effects across cyberspace. These two agencies initial responsibility was the protection of DOD networks only. But as early as 2012, both have pushed to expand their role beyond just protecting military networks to protecting private-sector networks from cyber-attacks.[20]

The Department of Justice (DOJ) has also begun using cyberspace to gather information intelligence. Flying small civilian aircraft with electronic boxes to mimic mobile communications towers, the DOJ is collecting location and unique registration information on tens of thousands of American citizens without their knowledge. This program eliminates prior need to cooperate with civilian corporations, and while court orders are obtained for these activities, it is not clear if the methods or span of collections are known when being approved as the orders are classified and sealed.[21]

New and innovative plans and strategies were put into action with regards to cyberspace, however the current political and social audiences have

had little to nothing to do with their creation. The US offensive cyber posture "offer[s] unique and unconventional capabilities to advance the US national objectives around the world with little or no warning…with potential effects ranging from subtle to severely damaging."[22] Unfortunately this strategy came to the public light only after it was implemented in the top-secret Presidential Policy Directive 20.[23] This incident raises concerns of possible uses of cyberspace that congressional leadership are unaware of. With what authority are actions within cyberspace actually being directed?

United States policy for cyberspace has continually lagged behind that needed since its inception. From 2002 to 2012, Congress held upwards of 60 hearings per year on the subject of cyberspace, but as of this writing no meaningful cyberspace legislation has passed.[24] The domain of cyberspace is predominately civilian; however, the majority of cybersecurity in the United States is performed by the NSA and USCYBERCOM. Authorities for cyberspace do not stem from the legislative branch of government—the representatives of society—but from the executive branch of government.

Before 9/11, the Federal Intelligence Surveillance Act of 1978 provided congressional authorization for electronic surveillance within the United States for national security purposes. Executive order 12333 placed additional restrictions on collection activities executed by the NSA. Most importantly, these collection activities required authorization from a Federal Intelligence Surveillance Court (FISC) within the judicial branch.[25] These two documents

provided a balance of power between the legislative, executive, and judicial branches.

After the attacks on 9/11, the NSA began executing highly classified intelligence activities authorized in one highly classified Presidential Authorization now known as the President's Surveillance Program (PSP) without requiring FISC approval. [26] The judicial branch was removed from the approval of collections, specifically in the cyber domain. Shortly after this, President Bush established the Comprehensive National Cybersecurity Initiative providing the Department of Homeland Security with capabilities and authorities to protect against future cyber-attacks. This document points to an executive civilian agency, but themes running through it include phrases such as: "establish a 'front line of defense' against existing threats;" "defend against the full spectrum of threats through counterintelligence;" and, "develop strategies to deter malicious activities." These themes were continuations from previous military documents and strategies.[27]

Today trends in industry are driving increased utilization of civilian corporations in the centralization and militarization of the domain. Recent attacks on businesses such as Sony, Target, and JPMorgan Chase have brought forth the creation of the Cyber Threat Intelligence Integration Center. The new center reports to the Director of National Intelligence and centralizes and integrates military, intelligence, and private sector cybersecurity efforts.[28]

It is difficult to gauge the full reach of the DOD in cyberspace since much of the policy around it is classified. In reviewing authorities and actions of the

PSP, and taking into light recurrent themes through strategies above, it is interesting to evaluate the environment of the garrison domain against Samuel Fitch's garrison state practices; manipulation of international crises, restriction of civil and political liberties for national security, and centralization of power in a militarized elite.[29] From the previous definition of powerful, it can be argued the DOD has both the power and the authority currently in cyberspace, but what about the influence?

Focus of Cyber Technology Production Towards War

Influence is the ability to get people to do what you want by convincing them it is in their best interests. In 2012, Secretary of Defense Leon Panetta warned the United States was facing a "cyber Pearl Harbor" threat from hackers who would destroy transportation systems, power grids, and financial and government networks.[30] By 2013 there were over a half-million references online to "cyber Pearl Harbor" and a quarter-million to a "cyber 9/11."[31] In 2013 the DOD's budget mentioned the threat from cyber 53 times; in 2014 it was mentioned 147 times.[32] The perceived threat from cyberspace and the prevalence of DOD within the domain makes it in the best interest for the industrial base, military, and research institutions to focus on militarization of cyberspace.

President Dwight Eisenhower warned of the military industrial complex whose "total influence—economic, political, even spiritual—is felt in every city, every state house, every office of the federal government."[33] Today the cyber

warfare industry is poised to be in the same position. Unlike wars in the physical domains, cyber war will never end; this means the opportunity for profits from a cyber warfare industry are endless. The cybersecurity industry is a $65 billion business projected to grow to $165 billion in the next ten years, leading to an increase in lobbying of Congress.[34] In 2001 there were four companies lobbying on cybersecurity issues, in 2012 there were 1,489.[35] The amount of focus towards cybersecurity and cyber war will not likely decrease so long as vulnerabilities in military, government, and civilian systems exist.

With the government, military, and industrial base focused on cybersecurity, the research and education institutions have also turned to the production of cybersecurity skills. The NSA sponsored National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD) promote higher education in IA and CD focusing on reducing cybespace vulnerabilities. There are currently 182 higher education institutions accredited by the NSA to study cybersecurity issues.[36]

The increase in industry's cybersecurity focus and capabilities runs counter to the capabilities and production of cyberspace for society. In 2000, only 4.4 percent of households in the United States had connectivity to broadband services. By 2010 homes with broadband service increased to 64 percent, with 94 percent of those only having the baseline speed of 10Mbps. From 2010 to 2012 the availability of commercial broadband connectivity to the civilian population only grew 36 percent for a single level of service. The

growth of broadband connectivity beyond the baseline speed has averaged only 25 percent from 2010 to 2012.

Although broadband service has made progress in expanding availability, growth is inconsistent across the country, specifically in rural areas. While basic 3Mbps broadband service is available almost everywhere, most Internet requirements outstrip this service speed. Additionally, as speeds increase gaps in availability between urban and rural widen, but availability overall decreases regardless.[37]

The perception of grave threats to society from cyberspace, and increased influence from the DOD, has focused the industrial base towards production of cyber warfare technology. Additionally, the nation's higher education institutions are also focusing on producing cyber warfare skillsets based on standards set by the NSA. Finally, comparisons between cyber warfare production and civilian cyberspace capability shows a distinct leaning towards cyber warfare production.

From Garrison Domain to Garrison State

The construct of a garrison domain and its impact outlined above would be disastrous, but what is the implication of a garrison domain for the state? The United States is wholly dependent on the existence of, and access to, the cyberspace domain. Citizens are uploading nearly every aspect of their lives to cyberspace. Some of this is compulsory, as government directs the transition to digital records increased efficiency, but a majority of uploading of personal

information is voluntary. The potential for a garrison domain to simplify transition to a garrison state increases as society continues to increase dependence on the cyberspace domain.

In Lasswell's article entitled, "The Universal Peril," soldiers and policemen begin as advisors to the civilian arm of government. However, in the presence of a persistent threat, and under the guise of security, restrictions are imposed by the soldier on the free flow of information and freedoms of speech. Preemptive surveillance and investigation is employed to identify those who might possibly be disloyal or dangerous to the state. Laws designed to protect civil liberties and freedoms are more often violated than kept, and the government supports this violation. Public opinion becomes less informed due to restrictions in the flow of information and is therefore viewed as less important. The powers of the legislative and judicial branches of government become weak in relation to the executive branch, elections degenerate into polls and surveys, and civilian agencies are finally supplanted by military agencies.[38]

Lasswell's example above, and the consequences of militarization averred in the early 20th century, can now be accomplished solely through the cyberspace domain. Arguably, some of the results of militarization have occurred in the cyberspace domain and their effects on the state are as Lasswell predicted. The DOD and DOJ currently act as advisors to the executive and legislative branches of government. In the name of security the transparency of DOD, intelligence, and law enforcement agencies is being reduced. Many of the programs, capabilities, threats, actions, and decisions

made in cyberspace are highly classified and hidden from public review. Recent revelations from leaks of classified information paint a picture of wide-ranging surveillance and violation of Fourth Amendment rights of American citizens, all executed under classified presidential directives that preempt participation of the legislative and judicial branches. Finally, the presidential directives, classification of operations, and efforts at the highest levels have reduced the ability of Congress and the Supreme Court to implement proper checks and balances on the executive branch. The almost total dependence of modern US society on the cyberspace domain and its perceived militarization appears to be easing the nation's transition to a garrison state as Lasswell outlined in his 1941 construct.

Counter Arguments

Samuel Huntington's book, *The Soldier and The State*, written post-World War II, was predicated by the smaller drawdown, as compared to previous wars, of the United States' large standing military.[39] The potential threat of a new conflict with the Soviet Union, and existential threat of nuclear war, changed America's liberal view on standing armies; from aversion to necessity. In his book, Huntington argued that Lasswell's theory was based on misconceptions of military predispositions and values. Unlike its civilian counterparts, Lasswell saw the military fraught with a desire for war. Huntington critiqued Lasswell's discrete view of either a peaceful, utopian, one-world society, or total war and destruction. Huntington's theory of civil-

military relations allowed for adjustment to strife and disagreement based on an aversion to war. In the end he saw Lasswell's construct of a garrison state as a misconception in identification of military control as a form of government vice a relationship between civilian and military leaders.[40]

Huntington's argument works well in the physical world because of aversion to violence and the professionalism of the military officer; however, his argument doesn't work as well, if at all, in cyberspace due to the lack of direct violence against society. The lack of physical violence reduces the necessity to adjust based on friction and strife making it easier for the domain to slide into a garrison existence. Additionally, societal requirements to be part of the domain simplify the transition to a garrison state, with society not realizing it until it is too late. Finally, even with a professional military, the transition to a garrison domain may be so subtle even specialists on information would be unaware until it is too late. The threat and lack of violence inherent to cyberspace may present to daunting a perceived risk to the nation to allow for any other course of action.

Conclusion

The limit and span of cyberspace is unknown yet constantly changing. Without addressing data and issues currently classified it is difficult to say with any certainty that we are approaching a garrison domain in cyberspace and why. This new domain does not conform to the physical world like the other domains, which makes applying or mirroring concepts from the physical

world difficult if not impossible. Compounding these difficulties is the highly technical and specialized nature of cyberspace. The result is a nebulous, ever changing concept difficult for experts, much less average Americans, to understand.

According to Fitch, a high level of professionalism within the US military would make it unlikely for there to be support for a garrison state scenario unless a threat to national security perceived as grave or existential existed.[41] The United States strives to maintain balanced civil-military relations, but the new domain of cyberspace has introduced a method, or pathway, to attack the US at the speed of light. This creates a persistent threat, real or perceived, and the power to defend against this threat currently resides in the DOD. The omnipresence and action of the DOD within cyberspace exhibit some of the garrison state traits described by Lasswell, and while Huntington's theory of civil-military relations allowed for adjustment to strife and disagreement, it was based on an aversion to war.

War in Huntington and Lasswell's time was violence on a global scale, and the desire to avoid war and violence was almost universal. The international community has yet to define what an act of war in cyberspace would look like and in cyberspace violence does not exist. Because of this there might not be as much incentive for military and civilian entities to adjust to strife and difficulty in the cyberspace domain. Assuming no incentives exist, and actions within cyberspace are capable of producing effects but not violence

in the physical domains, cyberspace could become a garrison domain and, in-turn, result in a garrison state environment in the physical world.

The academic and policy studies available regarding civil-military relations were mostly written in a pre-cyber world; a world where actions and results are governed by Newtonian physics within time and space. As mentioned above, cyberspace pervades all aspects of life, policy, and war, and is not subject to the restrictions of physical domains. Therefore, it is vital senior military leaders and political decision makers understand the impacts of the cyberspace domain not only from a warfare perspective, but also from a civil-military relations perspective, and adjust laws and policies accordingly to restore the checks and balances of power in the cyber domain.

Notes

1. Harold D. Lasswell, *Essays on the Garrison State*, Edited by Jay Stanley, New Brunswick, NJ: Transaction Publishers, 1997, 56.
2. Ibid., 56.
3. Angelle A. Khachadoorian, interview by Shannon Cummins, 2015, Cultural Studies 503: Political Culture (March 26).
4. Ibid., 22.
5. Ibid., 23-24.
6. Ibid., 55, 69.
7. Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, Joint Publication, Washington D.C.: Department of Defense, 2010, 63.
8. James Madison, *Selected writings of James Madison,* Edited by Ralph Ketcham, Indianapolis, IN: Hackett Publishers, 2006, 236.
9. Nicco Mele, *The End of Big: How the Internet Makes David the New Goliath*, First edition, New York: St. Martin's Press, 2013, 155.
10. Harold D. Lasswell, *Essays on the Garrison State,* Edited by Jay Stanley, New Brunswick, NJ: Transaction Publishers, 1997, 60-64.
11. Thomas Rid, *Cyber War Will Not Take Place,* New York: C. Hurst & Co Ltd., 2013, 15-18.
12. Harold D. Lasswell, *Essays on the Garrison State,* Edited by Jay Stanley, New Brunswick, NJ: Transaction Publishers, 1997, 34.
13. Ibid., 69-71.
14. Robert J. Carey, "DoD CIO Priorities for 2014," Washington, D.C.: Department of Defense, 2014, slide 5.
15. Department of Defense, 2013, *DoD Strategy for Defending Networks, Systems, and Data.* Washington, D.C.: Department of Defense, 5.
16. Goldman, David. 2013. *CNN Money.* January 9. Accessed March 21, 2015. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/. and P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York, NY: Oxford University Press, 2014, 96.
17. Lisa Ferdinando, 2015, "Dempsey: Cyber Vulnerabilities Threaten National Security," *DoD News*, January 21.
18. Symantec, 2014, *Internet Security Threat Report 2014: Volume 19,* Security Report, Mountain View: Symantec Corporation, 13.
19. Keith B. Alexander, 2010, *Statement of Commander United States Cyber Command before the House Committee on Armed Services,* Washington, D.C.: Department of Defense, 1.
20. Ellen Nakashima, "White House, NSA weigh cybersecurity, personal privacy," Washington Post, February 27, 2012: n.p.

21. Devlin Barrett, "Americans' Cellphones Targeted in Secret US Spy Program," *The Wall Street Journal*, November 13, 2014: n.p.
22. P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York, NY: Oxford University Press, 2014, 275.
23. Glenn Greenwald and Ewen MacAskill, 2013, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian*, June 7. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.
24. P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York, NY: Oxford University Press, 2014, 198.
25. Offices of the Inspector General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence. "Unclassified Report on the President's Surveillance Program." Washington, D.C., 2009, 4.
26. Ibid., 5-6.
27. Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace.* Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013, 5-6.
28. Tom Risen, 2015, "New Agency to Aid in Battle Against Hackers," *US News*, February 10, http://www.usnews.com/news/articles/2015/02/10/new-cybersecurity-agency-to-aid-in-battle-against-hackers.
29. Samuel J. Fitch, "The Garrison State in America," 33.
30. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on US" *The New York Times*, October 11, 2012: n.p.
31. P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York, NY: Oxford University Press, 2014, 37.
32. Ibid., 134-135.
33. Shane Harris, 2014, *@War: The Rise of the Military-Internet Complex,* New York: Houghton Mifflin Harcourt Publishing Company, 218.
34. P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York, NY: Oxford University Press, 2014, 162-163.
35. Ibid., 164.
36. National Security Agency, 2015, *National Centers of Academic Excellence in Information Assurance (IA)/ Cyber Defense (CD),* March 27, Accessed March 27, 2015, National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).
37. National Telecommunications and Information Administration. *US BROADBAND AVAILABILITY: JUNE 2010 – JUNE 2012.* National Telecommunications and Information Administration, 2013, 15.
38. Harold D. Lasswell, *Essays on the Garrison State,* Edited by Jay Stanley, New Brunswick, NJ: Transaction Publishers, 1997, 118.

39. Samuel P. Huntington, *The Sodier and the State.* Cambridge, MA: Harvard University Press, 1957

40. Samuel P. Huntington, *The Sodier and the State.* Cambridge, MA: Harvard University Press, 1957, 346-350.

41. Samuel J. Fitch, "The Garrison State in America: A Content Analysis of Trends in the Expectation of Violence," *Journal of Peace*, March 1985: 31-45, 32.

BIBLIOGRAPHY

Alexander, Keith B. 2010. *Statement of Commander United States Cyber Command before the House Committee on Armed Services.* Washington, D.C.: Department of Defense.

AV-TEST. 2014. *Malware.* March 24. Accessed March 24, 2014. http://www.av-test.org/en/statistics/malware/.

Barrett, Devlin. 2014. "Americans' Cellphones Targeted in Secret US Spy Program." *The Wall Street Journal*, November 13: n.p. Accessed November 17, 2014. http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

Bumiller, Elisabeth, and Thom Shanker. 2012. "Panetta Warns of Dire Threat of Cyberattack on US" *The New York Times*, October 11: n.p. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Bureau of Justice Statistics. n.d. *Terms & Definitions: Law Enforcement.* Accessed February 19, 2015. http://www.bjs.gov/index.cfm?ty=tdtp&tid=7.

Bush, George W. 2003. *National Strategy to Secure Cyberspace.* Washington, D.C.: White House.

Carey, Robert J. 2014. "DoD CIO Priorities for 2014." Washington, D.C.: Department of Defense. http://www.slideshare.net/GTSCoalition/robert-carey-principal-cio.

Chairman of the Joint Cheifs of Staff. 2006. *National Military Strategy for Cyberspace Operations.* Washington, D.C.: Department of Defense.

Chen, Thomas M. 2013. *An Assessment of the Department of Defense Strategy for Operating in Cyberspace.* Carlisle, PA: Strategic Studies Institute and US Army War College Press.

Choucri, Nazli, and David D. Clark. 2013. "Who controls cyberspace?" *Bulletin of the Atomic Scientists, Vol. 69 Issue 5* 21-31.

Clodfelter, Mark. 1989. *The Limits of Air Power.* London: Collier Macmillan Publishers.

Darmer, M. Kathrine B., Robert M. Baird, and Stuart E. Rosenbaum, . 2004. *Civil Liberties vs. National Security in a Post-9/11 World.* New York: Prometheus Books.

Defense Science Board. 2013. *Resilient Military Systems and the Advanced Cyber Threat.* Task Force Report, Washington, D.C.: Department of Defense.

DeNardis, Laura. 2014. *The Global War for Internet Governance.* New Haven: Yale University Press.

Department of Defense. 2013. *Cyberspace Workforce Strategy.* Washington, D.C.: Department of Defense.

Department of Defense. 2013. *DoD Strategy for Defending Networks, Systems, and Data.* Washington, D.C.: Department of Defense.

Department of Defense. 2010. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms.* Joint Publication, Washington D.C.: Department of Defense.

Douhet, Giulio. 1998. *The Command of the Air.* Washington, D.C.: Air Force History and Museums Program.

Dunn Cavelty, Myriam. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review, Vol. 15 Issue 1* 105-122.

Ferdinando, Lisa. 2015. "Dempsey: Cyber Vulnerabilities Threaten National Security." *DoD News*, January 21.

Fisher, Louis. 2008. *The Constitution and 9/11: Recurring Threats to America's Freedoms.* Lawrence: University of Kansas.

Fitch, Samuel J. 1985. "The Garrison State in America: A Content Analysis of Trends in the Expectation of Violence." *Journal of Peace*, March: 31-45. Accessed October 1, 2014. http://www.jstor.org.aufric.idm.oclc.org/stable/view/423584?&Search=yes&searchText=The&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DThe%2Bgarrison%2Bstate%2Bin%2BAmerica%26amp%3Bacc%3Don%26amp%3Bwc%3Don%26amp%3Bfc%3Doff.

Goldman, David. 2013. *CNN Money.* January 9. Accessed March 21, 2015. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/.

Goth, Gregory. 2009. "US Unveils Cybersecurity Plan." *Communications of the ACM, Vol. 52 Issue 8* 23.

Greenwald, Glenn, and Ewen MacAskill. 2013. "Obama orders US to draw up overseas target list for cyber-attacks." *The Guardian*, June 7.

http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Gruenspecht, Joshua. 2013. "Cyber Security and Identity: Solutions for Critical Infrastructure that Protect Civil Liberties and Enhance Security." In *Cyber Infrastructure Protection Vol. II*, edited by Tarek Saadawi, Louis H. Jordan, Jr. and Vincent Boudreau, 139-182. Carlisle, PA: US Army War College Press.

Guarino, Alessandro. 2013. "THE STATE VS THE PEOPLE." *Engineering & Technology, Vol 8 Issue 10* 43-45.

Harris, Shane. 2014. *@War: The Rise of the Military-Internet Complex.* New York: Houghton Mifflin Harcourt Publishing Company.

Headquarter United States Air Force. n.d. "USCYBERCOMMAND Cyber Mission Force." *SAF CIO A6: Information Dominance.* Accessed March 26, 2015. http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf.

Huntington, Samuel P. 1957. *The Soldier and the State.* Cambridge, MA: Harvard University Press.

Khachadoorian, Angelle A., interview by Shannon Cummins. 2015. *Cultural Studies 503: Political Culture* (March 26).

Lasswell, Harold D. 1941. "The Garrison State." *American Hournal of Sociology, Vol 46 Issue 4.* 455-468.

Lasswell, Harold. 1997. *Essays on the Garrison State.* Edited by Jay Stanley. New Brunswick, NJ: Transaction Publishers.

Libicki, Martin C. 2007. *National Security and Information Warfare.* New York: Cambridge University Press.

Madison, James. 2006. *Selected writings of James Madison.* Edited by Ralph Ketcham. Indianapolis, IN: Hackett Publishers.

Mele, Nicco. 2013. *The End of Big: How the Intenet Makes David the New Goliath.* First Edition. New York: St. Martin's Press.

Menn, Joseph. 2014. "Exclusive: NSA infiltrated RSA security more deeply than thought - study." *Reuters.* http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331.

Merriam-Webster. 2014. *Merriam-Webster.* November 5. Accessed November 5, 2014. http://www.merriam-webster.com/dictionary/domain.

Nakashima, Ellen. 2012. "White House, NSA weigh cybersecurity, personal privacy." *Washington Post*, February 27: n.p.

National Security Agency. 2015. *National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).* March 27. Accessed March 27, 2015. National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).

National Telecommunications and Information Administration. 2013. *US BROADBAND AVAILABILITY: JUNE 2010 – JUNE 2012.* National Telecommunications and Information Administration.

Obama, Barack H. 2011. *International Strategy for Cyberspace.* Washington, D.C.: The White House.

Offices of the Inspector General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence. 2009. "Unclassified Report on the President's Surveillance Program." Washington, D.C.

O'Harrow Jr., Robert W. 2005. *No Place to Hide.* New York: Free Press.

Owens, Mackubin Thomas. 2011. *US Civil-Military Relations After 9/11: Renegotiating the Civil-Military Bargain.* New York, NY: The Continuum International Publishing Group.

Pellerin, Cheryl. 2013. "Alexander: Defending Against Cyberattacks Requires Collaboration." *DoD News*, October 30. http://www.defense.gov/news/newsarticle.aspx?id=121030.

PricewaterhouseCoopers LLP. 2011. *Cyber Security M&A: Decoding deals in the Global Cyber Security Industry.* PricewaterhouseCoopers LLP. Accessed November 27, 2014. http://www.pwc.com/en_GX/gx/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf.

Rid, Thomas. 2013. *Cyber War Will Not Take Place.* New York: C. Hurst & Co Ltd.

Risen, James, and Eric Lichtblau. 2005. "Bush Lets US Spy on Callers Without Courts." *The New York Times*, December 16.

Risen, Tom. 2015. "New Agency to Aid in Battle Against Hackers." *US News*, February 10. http://www.usnews.com/news/articles/2015/02/10/new-cybersecurity-agency-to-aid-in-battle-against-hackers.

Rosenzweig, Paul. 2013. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World.* Santa Barbara, CA: Praeger.

Sharp Sr., Walater Gary. 1999. "Balancing Our Civil Liberties with Our National Security Interests in Cyberspace." *Texas Review of Law and Politics* 69-75.

Sheldon, John B. 2012. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Edited by Derek S. Reveron. Washington, D.C.: Georgetown University Press.

Singer, P. W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York, NY: Oxford University Press.

Stone, Geoffrey R. 2007. *War and Liberty.* New York: W. W. Norton & Company.

Symantec. 2014. *Internet Security Threat Report 2014: Volume 19.* Security Report, Mountain View: Symantec Corporation.

White Hosue. n.d. *Comprehensive National Cybersecurity Initiative.* Washington, D.C.: The White House. Accessed November 17, 2014. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Williams, Brett. 2014. "Cyberspace: What is it, where is it and who cares? ." *Armed Forces Journal*, March 13: n.p.