ROUTLEDGE STUDIES IN CONFLICT, SECURITY AND TECHNOLOGY

International Conflict and Cyberspace Superiority

Theory and practice

William D. Bryant

ROUTLEDGE

International Conflict and Cyberspace Superiority

Theory and practice

William D. Bryant

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2016
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Bryant, William D. (Career Fighter Pilot)
International conflict and cyberspace superiority : theory and practice / William D. Bryant.
pages cm. — (Routledge studies in conflict, security, and technology)
Includes bibliographical references and index.
ISBN 978-1-138-91891-7 (hardback : alk. paper) — ISBN 978-1-315-68818-3 (ebook : alk. paper) 1. Cyberspace—Political aspects. 2. Social conflict.
I. Title.
HM851.B79 2015
303.48'34—dc23 2015006411

ISBN: 978-1-138-91891-7 (hbk)
ISBN: 978-1-315-68818-3 (ebk)

Typeset in Baskerville MT
by Keystroke, Station Road, Codsall, Wolverhampton

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C013056

Printed and bound in Great Britain by
TJ International Ltd, Padstow, Cornwall

International Conflict and Cyberspace Superiority

This book examines cyberspace superiority in nation-state conflict from a theoretical and a practical perspective.

This book analyzes superiority concepts from the domains of land, maritime, and air to build a model that can be applied to cyberspace. Eight cyberspace conflicts between nation-states are examined and the resulting analysis is combined with theoretical concepts to present the reader with a conclusion. Case studies include the conflict between Russia and Estonia (2007), North Korea and the U.S. and South Korea (2009) and Saudi Arabia and Iran in the Aramco attack (2012). The book uses these case studies to examine cyberspace superiority as an analytical framework to understand conflict in this domain between nation-states. Furthermore, the book makes the important distinction between local and universal domain superiority, and presents a unique model to relate this superiority in all domains, as well as a more detailed model of local superiority in cyberspace. Through examining the eight case studies, the book develops a rigorous system to measure the amount of cyberspace superiority achieved by a combatant in a conflict, and seeks to reveal whether cyberspace superiority proves to be a significant advantage for military operations at the tactical, operational, and strategic levels.

This book will be of much interest to students of cyber conflict, strategic studies, national security, foreign policy and IR in general.

William D. Bryant is a career fighter pilot and has a PhD from the School of Advanced Air and Space Studies, Maxwell, USA.

Routledge Studies in Conflict, Security and Technology

Series Editors: Mark Lacy, Dan Prince, Sylvia Walby and Corinne May-Chahal, *Lancaster University*

The *Routledge Studies in Conflict, Security and Technology* series aims to publish challenging studies that map the terrain of technology and security from a range of disciplinary perspectives, offering critical perspectives on the issues that concern public, business and policymakers in a time of rapid and disruptive technological change.

Nonlinear Science and Warfare
Chaos, complexity and the U.S. military in the information age
Sean T. Lawson

Terrorism Online
Politics, law, technology
Edited by Lee Jarvis, Stuart Macdonald and Thomas M. Chen

Cyber Warfare
A multidisciplinary analysis
Edited by James A. Green

The Politics of Humanitarian Technology
Good intentions, unintended consequences and insecurity
Katja Lindskov Jacobsen

International Conflict and Cyberspace Superiority
Theory and practice
William D. Bryant

Figures

2.1 General Model of Gaining and Utilizing Domain Superiority 13
2.2 Generic Model of Domain Superiority Split into Offensive and Defensive 14
2.3 Model of Gaining and Utilizing Land Superiority 19
2.4 Model of Gaining and Utilizing Maritime Superiority 28
2.5 Model of Gaining and Utilizing Air Superiority 38
3.1 Libicki's Model of Cyberspace 54
3.2 Model of Gaining and Utilizing Cyberspace Superiority 65
4.1 Domain Means, Ways, and Ends 85
4.2 Domain Means and Ways with Defensive Block 86
4.3 Domain Superiority Model 86
4.4 Cyberspace Means and Ways 103
4.5 Model of Local Cyberspace Superiority with Defensive Blocks 113
4.6 Complete Model of Local Cyberspace Superiority 117
5.1 Effects Component Summary 127
6.1 Russia versus Estonia 2007 Local Cyberspace Superiority Model 143
6.2 Russia versus Georgia 2008 Local Cyberspace Superiority Model 147
6.3 North Korea versus South Korea/U.S. 2009 Local Cyberspace Model 150
6.4 Stuxnet Local Cyberspace Model 155
6.5 North Korea versus South Korea DDoS 2011 Local Cyberspace Model 158
6.6 North Korea versus South Korea Bank Attack 2011 Local Cyberspace Model 161
6.7 Aramco Attack Local Cyberspace Model 164
6.8 North Korea versus South Korea Bank Attack 2013 Local Cyberspace Model 167
7.1 Domain Conflict Model 196
7.2 Local Cyberspace Superiority Model 197

Tables

2.1 Summary of Domain Superiority for Land, Maritime, and Air Domains 45
3.1 Summary of Domain Superiority Characteristics 76
6.1 Cyberspace Superiority Case Studies 169
7.1 Summary of Domain Characteristics and Domain Superiority 193
7.2 Summary of Cyberspace Superiority Case Studies 198
A.1 Level of Success (S) Coding 205
A.2 Level of Functionality (L) Coding 207
B.1 Russian Objectives in Estonian Attack 211
B.2 Estonian Systems under Attack in 2007 211
B.3 Russian Offensive Objectives in Russian/Georgian Conflict 213
B.4 Georgian Offensive Objectives in Russian/Georgian Conflict 214
B.5 Critical Russian Systems in Russian/Georgian Conflict 214
B.6 Critical Georgian Systems in Russian/Georgian Conflict 216
B.7 North Korean Offensive Objectives in 2009 218
B.8 Critical U.S. and South Korean Systems in 2009 218
B.9 U.S./Israeli Objectives with Stuxnet versus Iran 221
B.10 Iranian Systems in Stuxnet Attack 222
B.11 North Korean Offensive Objectives in 2011 DDoS Attack 224
B.12 Critical U.S. and South Korean Systems in 2011 DDoS Attack 225
B.13 North Korean Offensive Objectives in 2011 Bank Attack 227
B.14 Critical South Korean System in 2011 Bank Attack 227
B.15 Iranian Objectives in Aramco Attack 229
B.16 Saudi Arabian Systems in Aramco Attack 230
B.17 North Korean Offensive Objectives in April 2013 Attack 231
B.18 Critical South Korean Systems in April 2013 Attack 232

Contents

List of Figures vii
List of Tables ix

1 Introduction 1

2 Elements of Domain Superiority from the Other Domains 11

3 Cyberspace Domain Characteristics 51

4 Local Cyberspace Superiority 83

5 Measuring Cyberspace Superiority 124

6 Cyberspace Superiority Case Studies 136

7 Conclusion 183

Appendix A: Coding of Measurement Inputs 204

Appendix B: Cyberspace Superiority Case Study Measurement 210

Index 236

1 Introduction

The importance of cyberspace continues to grow in the modern world. Now it is not just the computer under the desk that is part of cyberspace. We are connecting our cars, phones, kitchen appliances, and even toilets to cyberspace. These connections allow increases in functionality and productivity unimaginable even in the realm of science fiction just a few years ago. Today's iPhone makes a "Star Trek" communicator look like a caveman's rock abacus, but the iPhone is the one that actually exists. Unfortunately, just like a "Star Trek" ship's computer runs amok, our devices may be working against us.

There is a dark side to this ever-increasing connectivity and functionality. Our iPhone can be spying on us and reporting our every move to a foreign intelligence service, our car might be reporting our location to an enemy, and malicious hackers can even take over our humble toilet to humiliate us.[1] Action from cyberspace is not only limited to malicious pranks. Hackers have demonstrated the ability to send potentially lethal commands to common cars, such as the Toyota Prius. One pair of enterprising hackers has demonstrated the capability to blast the horn uncontrollably, "make pathological liars out of speedometers and odometers," spoof the GPS, and even violently jerk a Prius' steering at any speed, threatening a potentially lethal collision.[2] These threats and vulnerabilities become even more magnified as you look at cyberspace systems on the municipal or national level.

Cyberspace is increasingly becoming an arena for nation state conflict. If a nation were to drop a bomb on an enemy power plant, the target nation would consider it an act of war. If the same nation sent a "logic bomb" through cyberspace causing the same amount of damage to the power grid, that is also war. The delivery method does not change the physical effect of the attack. Analysts are increasingly accepting cyberspace as a domain, or discrete region, where combatants fight, much like the domains of land, maritime, air, and space. According to former National Security Council Director for Cyber Security, Gregory Rattray, a goal of U.S. national strategy is to gain control of cyberspace.[3] The nature of warfare has not changed, but now there is a new field to fight on, much like when aircraft first opened up the air domain to warfare in the early 1900s. Although the majority of analysts have accepted cyberspace as a domain of warfare, there are some dissenting voices.

I agree with the majority of analysts who think that treating cyberspace as a domain is useful. One well known analyst that takes the opposing view is Martin Libicki who proposes that thinking of cyberspace as a domain causes cyberspace operators to apply inappropriate "warfighting" concepts at the expense of other paradigms such as systems engineering.[4] There are many reasons I think warfighting is a better mental template for conflict in cyberspace than systems engineering or any other proposed construct, but the most important is that cyberspace conflict is fundamentally human conflict in a new medium. Computers are not attacking each other and trying to steal other computer's information, people are attacking each other and trying to steal other people's information using computers. This means that the classic illustration of conflict by Carl von Clausewitz of two wrestlers dynamically reacting to each other applies as much in cyberspace as in the other physical domains.[5] I contend that thinking of cyberspace as a warfighting domain is far more helpful than thinking of it as an engineering problem and I will more fully develop this topic throughout this book. Some analysts don't argue that cyberspace is not a domain, they instead argue that war in cyberspace will not happen.

Thomas Rid's basic thesis is that "cyber war" has not happened, is not happening, and will not happen in the future.[6] Rid's thesis is completely dependent upon his definition of "cyber war," which he defines as having to include the potential to be lethal, "at least for some participants on at least one side."[7] I agree with Rid that cyber weapons will not often be the proximate cause of death, although there are a number of scenarios such as crashing a drone into a building where they could be.[8] I do not agree with Rid that the fact that people are generally not directly killed by cyberspace weapons means we should not think of conflict in cyberspace using theories from warfare. I am also not sure how relevant it is to soldiers who are killed when their positions are overrun because they lost all ability to communicate or call in fire support.

Normally, death and destruction will be dealt out through the physical domains, but that is increasingly facilitated and supported through the cyberspace domain. As a result of its importance, "war" has already started in cyberspace, although I use the term "conflict" to help identify that it is normally not as violent as in the other domains. If cyberspace is different from the other domains in that it is less violent, how else is it different? What is the basic character of this new domain?

Cyberspace is difficult to grasp intuitively because we cannot experience it directly with our senses. We can stand on the land, dive into the water, and see aircraft or satellites with our eyes. To "see" cyberspace we rely on computer screens or diagrams that provide representations, but we are not looking at or experiencing cyberspace directly. Another thing that makes cyberspace difficult to grasp is that it often operates inside or underneath the physical objects we see. According to Professor Chris Demchak, "orchestrating a national security response to cybered threats is hard because cyberspace is *hard to see physically* in any case, but especially so now as it is deeply embedded in normal societal functions."[9] Cyberspace underpins modern society and if it were seriously disrupted, only then would we understand what it had previously been doing for us. In that respect cyberspace in the modern world is like air; people take it for granted and do not think about its importance until it is no longer there. This difficulty in visualizing cyberspace makes careful definition of the domain even more important.

Connections between computing devices create cyberspace. An isolated computer sitting on a desk is no more part of the cyberspace domain than a ship sitting in dry dock is part of the maritime domain. The connections are what matter. The United States Joint Staff has defined 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."[10] Although this definition has achieved wide acceptance, one common area of misunderstanding is the relationship between cyberspace and the Internet.

Cyberspace and the Internet are not synonymous, the Internet is a smaller subset of the larger cyberspace. This understanding has important implications for conflict in cyberspace, but the idea of the Internet as cyberspace is widespread. Even Libicki states that, "The Internet is basically tantamount to cyberspace; everything connected to the Internet is connected to cyberspace and, therefore, part of cyberspace."[11] Although everything connected to the Internet is connected to cyberspace, that does not make the Internet tantamount to cyberspace as there are many interdependent networks of information technology infrastructures that are not part of the Internet. Some examples include air gapped systems such as Iran's nuclear enrichment facilities, as well as embedded processors and controllers in a range of platforms, from cars to satellites. The danger in thinking of cyberspace as the Internet is that non-Internet connected devices are ignored by cyberspace defenders focused on traditional networks, when often those systems are the most critical to protect. Cyberspace is broader than the traditional Internet, but it is not useful to cast it so broadly as to include the entire electromagnetic spectrum.

One point of the definition that analysts still debate is whether to include the electromagnetic spectrum as part of cyberspace. As analysts first developed the concept of cyberspace, some policy makers included the electromagnetic spectrum as cyberspace's "maneuver space."[12] However, over time the definition has narrowed "down to the physical network infrastructure used for transmitting and storing information."[13] Sean Butler gave the principal reason for this narrowing when he stated that,

> The ability to process, store, and exchange large amounts of information rapidly, using automated systems, is the defining characteristic of cyberspace—the physical methods are superficial. In fact, its logical or virtual nature, rather than its physical mechanisms, sets cyberspace apart from other domains.[14]

I find this argument compelling and so will use the narrower Joint Staff definition from *Information Operations* for cyberspace, which does not try to include the entire electromagnetic spectrum.[15] I present a much more detailed analysis of the characteristics of the cyberspace domain in Chapter 3. Now that we have a definition of cyberspace, is freedom of action within that domain significant?

If the cyberspace domain is a key component of modern warfare, then it follows that freedom of action within that domain is important. According to Air Force Doctrine Document (AFDD) 3–12,

> Freedom of action in the cyberspace domain enables our command, control, communication, computers, intelligence, surveillance, and reconnaissance capabilities. Our modern defenses, industrial base, and global commerce, as well as that of our nation's enemies, depend on free use of land, sea, air, space, and cyberspace. Leverage in cyberspace affords influence and control across all other domains. This leverage increases our forces' access, speed, reach, stealth, and precision.[16]

In other domains, and especially in the air and maritime domains, analysts refer to this freedom of action as domain superiority.

The United States Air Force presents a clear definition of cyberspace superiority in Air Force doctrine. According to AFDD 3–12, cyberspace superiority is, "The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[17] This definition is the one I will use for cyberspace superiority and it is important to note that cyberspace superiority has an offensive and defensive component. Understanding this dual nature is critical and AFDD 3–12 goes on to provide more context and expand on the simple definition.

> Cyberspace superiority may be localized in time and space, or it may be broad and enduring. The concept of cyberspace superiority hinges on the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects. "Supremacy" prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations. While "supremacy" is most desirable, it may not be operationally feasible. Cyberspace superiority, even local or mission-specific cyberspace superiority, may provide sufficient freedom of action to create desired effects. Therefore, commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort.[18]

I will explore a number of important elements in this definition. The first element encompasses the different levels of cyberspace superiority.

There is a wide range of possibilities of how much advantage a combatant can have in a given domain. Note that in the AFDD 3–12 section quoted previously, there are at least two words used to discuss friendly freedom of action, "superiority" and "supremacy." There are also a large number of terms that authors and thinkers have applied to advantage in a domain that includes command, control, supremacy, and superiority. Because authors often use these terms to mean different things, it can be confusing when comparing multiple works. "Sea control," "command of the sea," "maritime superiority," and "control of sea communications" are all similar concepts, but there is no generally accepted hierarchy or understanding of how each term relates to the others. Accordingly, in this project I use the single term of cyberspace superiority, while acknowledging that there will be different levels of cyberspace superiority from near parity among the combatants, to complete domination of all of cyberspace by one combatant. In many of the quotations from other authors throughout this project, they use other terms such as "command of the air" or "sea superiority" and I have not altered them. I consider each of them to refer to domain superiority in their domain, with the addition that sometimes they imply greater or lesser domain superiority, as in AFDD 3–12, which places cyberspace supremacy over cyberspace superiority. The range of strength of superiority that a combatant can achieve brings up the related question of how much superiority a combatant needs or should seek.

A combatant should be seeking just enough cyberspace superiority to achieve their objectives, because seeking too much superiority can be counterproductive and prevent the attainment of strategic or operational objectives. For a combatant to pursue domain superiority requires resources that they could have applied to other important objectives. In addition, if a combatant seeks too high a level of superiority, there can be significantly diminishing returns for the increased resources put toward solving the problem. For example, in the air domain a combatant may be able to reduce an enemy Integrated Air Defense System (IADS) to 50% effectiveness at a reasonable level of effort, but to get to 99% degradation will normally be cost prohibitive. Temporary, local superiority may be sufficient if that is all that is required to accomplish the mission or objective. For example, when the Israeli Air Force bombed the Iraqi nuclear reactor, they did not seek air supremacy or even air superiority over all of Iraq; they simply wanted air superiority over the target and the ingress and egress corridors for just long enough to destroy the reactor. The Israelis were very successful by only seeking just enough superiority to accomplish their mission; had they attempted to gain total air supremacy they would not have been able to, and would not have been able to destroy the reactor. On the other hand, some analysts think that even limited cyberspace superiority is not a useful concept or goal for military forces.

Analysts have a wide range of opinions on the utility of cyberspace superiority as a concept. Martin Libicki is a well-known cyberspace analyst who is rather blunt when he states that, "the question of cybersupremacy is meaningless and, as such, is not a proper goal for operational cyberwarriors."[19] Owens, Dam, and Lin are slightly more circumspect and see some utility for developing capabilities, but still say that conflict in cyberspace will be very different from in the land, air, and maritime domains, which will make enduring dominance of cyberspace by the United States unrealistic.[20] Cyberspace analyst Jeffrey Carr states that the tendency of U.S. military forces to attempt to control the domains they operate in is a problem for the United States as no nation can dominate or control cyberspace.[21] Carr is afraid that the United States will pour resources into seeking an objective that is not attainable. Professor David Lonsdale concurs with Carr that a high level of cyberspace superiority is not attainable. Lonsdale looks at Douhet's definition of command of the air and states that an equivalent command of cyberspace is impossible and even undesirable, as it would require denying an enemy effective use of their information assets.[22] Not all analysts agree that there is no value to the concept of cyberspace superiority; some see it as a useful concept that requires modification when applied to the new cyberspace domain.

What these objections highlight is that cyberspace is not like the other domains, which will make gaining superiority look different, and the character of the superiority gained may be different as well. This difference in character does not release the cyberspace warrior from attempting to control their domain. According to well-known strategic theorist Colin Gray,

> To make advantageous use of an army, navy, air force, space force, and information force, it is necessary as a prerequisite to seek out and defeat the geographically similar forces of the enemy. If use of the sea is vital to us, in consequence it is vital to an enemy that he should be able to contest our ability to use the sea. The same strategic logic applies to the air, to orbital space, and to cyberspace. The technologies, tactics, and operational aims must vary with what is feasible in each unique geographical environment: the strategic logic, however, is uniform.[23]

Gray's strategic logic will drive cyberspace operators to attempt to control the cyberspace domain even if it is difficult. We should not simply ignore cyberspace superiority, we should wrestle with it to determine whether there is utility for strategists and planners in the concept.

The purpose of this book is to closely examine the concept of cyberspace superiority to determine whether it is a useful construct for thinking about and planning for nation-state conflict in cyberspace. The argument I will develop is that cyberspace superiority does provide a useful construct, but it requires significant modification from superiority in the other domains to account for the unique characteristics of the cyberspace domain. As I examine the characteristics of the cyberspace domain compared to the other physical domains, I begin to frame several important questions that shape my analysis.

The first question is whether domain superiority is a local or universal concept. In the more familiar air domain, combatants often implement air superiority through combat air patrols, or CAPs, where fighter aircraft hold a position and deny that space to the enemy. However, a single flight of aircraft cannot fly to their assigned CAP, "plant the flag" and fly home having established air superiority over the entire theater of operations. They have only established air superiority in the area of the domain that their sensors and weapons can reach and only for as long as they are in their CAP. Nevertheless, the fact that they have established superiority in their local part of the air domain also affects the overall superiority in the theater air domain, as the enemy now cannot utilize the airspace occupied by the CAP without fighting for it. So what is the relationship is between local and universal superiority in the cyberspace domain? I examined how the local and universal levels of domain superiority interacted among the physical domains and found that in the cyberspace domain, the local level of superiority is dominant over the universal level. The analysts who state you cannot gain total "command of the cyber" are correct if you restrict cyberspace superiority to the universal level. It is on the local level where realistic cyberspace superiority can be sought and won. The simple example of a CAP in the air domain also highlights another issue.

The second question is how persistent domain superiority typically is. When the aircraft return to base, what happens to the air superiority that the combatant gained? Does it continue and persist? In the case of the CAP, once the aircraft return to base, the enemy can utilize the airspace just as easily as before the aircraft set up the CAP, so there is no longer superiority in that localized area. Accordingly, the combatant will have to rotate aircraft through the CAP so that there are always fighters on station if they desire persistent superiority. What does persistence look like in the cyberspace domain? After all, if the persistence of superiority in a domain is zero, then there cannot be superiority in that domain. Does the great speed of action in the cyberspace domain result in persistence so short that it makes cyberspace superiority not worth pursuing? After looking at domain superiority theory from the other domains, and sifting through the case study evidence, it is readily apparent that superiority in the cyberspace domain tends to be transitory, unless the fact that they are under attack can be hidden from defenders. However, short cyberspace superiority can be long enough to accomplish a combatant's objectives as shown by the case studies. Looking at the persistence of cyberspace superiority over time brought up the final issue.

To examine the persistence of cyberspace superiority over time, I needed to develop some way of measuring cyberspace superiority. Simply comparing the force structures of the two sides will not tell you definitively who has, or is likely to gain, superiority. If an analyst looked only at the aircraft and systems possessed by Israel and Syria before the Bekaa Valley air campaign of 1982, it would have given no indication of the extremely one-sided air superiority subsequently gained by the Israelis. However, there are useful metrics that combatants routinely utilize to measure air superiority. What percentages of friendly strike aircraft are successfully attacking their targets? How many enemy aircraft are getting through and hitting friendly targets? Which side is losing more aircraft? Often, the indicators will be mixed and hard to read during a campaign. In a few cases, the superiority is obvious, such as when the Iraqis completely ceded the air domain and buried their fighters in the sand to try to preserve them for the future.[24] Generally, measurement of superiority in the cyberspace domain is not so simple.

Measurement of the level of superiority in the cyberspace domain is extremely difficult. The cyberspace domain is less tangible than the physical domains and it is harder to count and compare cyberspace weapons to aircraft, ships, or infantry divisions. However, many of the same concepts will apply. What percentage of friendly cyberspace strikes got through enemy defenses? How successfully are friendly defenses holding off enemy cyberspace attacks? These are the key questions that formed the foundation of a methodology of measuring cyberspace superiority. I settled on a weighted preference analytical model that is presented in

Chapter 5. As with any weighted preference model, the coding methodology is critical and is presented in the appendices.

To lay out the evidence and analysis I start by examining the elements of domain superiority and persistence of superiority from other domains in Chapter 2. I also develop a general model that links universal and local domain superiority and apply it to the land, maritime, and air domains. In Chapter 3, I examine the characteristics of cyberspace to develop the elements of domain superiority as they apply to it. I also apply the general model linking universal and local domain superiority to cyberspace. In Chapter 4, I delve into the details of local cyberspace superiority and build a model of what the key elements are and how they are related to each other. Chapter 5 explains the measurement methodology that I apply to analyze the case studies in Chapter 6. Having demonstrated how cyberspace superiority contributes to military operations, the final chapter will summarize what was learned by this analysis of cyberspace superiority. I will start by examining what elements of domain superiority I can pull from the other physical domains.

Notes

[1] Trevor Mogg, "Smart Toilet Security Flaw Could Result in Nasty Surprise," *Fox News*, 5 August 2013. www.foxnews.com/tech/2013/08/05/smart-toilet-security-flaw

[2] Andy Greenberg, "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel (Video)," *Forbes*, 24 July 2013. www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video

[3] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 255.

[4] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol 8:2 (2012): 328.

[5] Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

[6] Thomas Rid, *Cyber War Will Not Take Place* (Amazon: Oxford University Press, 2013), Kindle Location 144.

[7] Rid, Cyber War Will Not Take Place, Kindle Location 194.

[8] Rid is dismissive of this possibility as he assumes, "it is very unlikely that such an attack could succeed against a more complex armed military drone in the field." Thomas Rid, *Cyber War Will Not Take Place* (Amazon: Oxford University Press, 2013), Kindle Location 441. Given the government and military services' record so far in cyberspace security, to assume that no enemy could possibly penetrate military cyberspace defenses on an armed drone, seems unwise.

[9] Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: The University of Georgia Press, 2011), 176.

[10] Joint Chiefs of Staff, Joint Operations, Vol. 3–13, *Information Operations*, 2012, II–9.

[11] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol 8:2 (2012): 323–324. In the same article, Libicki discusses how some of the connections are "intermittent and asynchronous" and gives examples such as Natanz or DoD's SIPRNET. Libicki thus extends his definition of the Internet to cover many systems not directly part of the normal Internet. The problem with using this approach is that the nuance is often lost on less careful readers and there are still connected computing systems that never connect to the Internet but are part of cyberspace.

[12] Michael W. Wynne, "Flying and Fighting in Cyberspace," *Air Space Power Journal*, Volume 21, no. 1 (2007): 6.

[13] Thomas David McCarthy, "Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development" (PhD diss., Fletcher School of Law and Diplomacy, 2012), 56.

[14] Sean C. Butler, "Refocusing Cyber Warfare Thought," *Air Space Power Journal* Volume 27, no. 1 (January–February 2013): 50.

[15] There are numerous definitions of cyberspace, Daniel Kuehl gives fourteen in a single article in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 26–27. What is common across the majority of the definitions is the idea of communication via connected computing devices. I use the Joint Staff definition as it is well known and I find it to be among the most complete without overreaching into the electromagnetic spectrum.

[16] Air Force Doctrine Document (AFDD) 3–12, *Cyberspace Operations. Change 1*, 15 July 2010, ii.

[17] AFDD 3–12, *Cyberspace Operations. Change 1*, 2.

[18] AFDD 3–12, *Cyberspace Operations. Change 1*, 2.

[19] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 141.

[20] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 39.

[21] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Beijing: O'Reilly Media, 2011), Kindle location 4089, chap. 11.

[22] David J. Lonsdale, *The Nature of War in the Information Age* (London: Frank Cass, 2004), 184.

[23] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 209.

[24] In the first Gulf War the Iraqis flew a number of aircraft to Iran for safekeeping. The Iranians subsequently refused to return them and they were lost to the Iraqis anyway. In the second Gulf War the Iraqis tried to preserve some of their aircraft by burying them to be dug up later, but as the war resulted in the collapse of Saddam's regime, that attempt proved useless as well.

Bibliography

Air Force Doctrine Document (AFDD) 3–12, *Cyberspace Operations*, Change 1. 30 November 2011.

Butler, Sean C. "Refocusing Cyber Warfare Thought." *Air Space Power Journal*, Volume 27, no. 1 (2013): 44–57.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Beijing: O'Reilly Media, 2011. Kindle edition.

Clausewitz, Carl von. *On War.* Edited and Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Demchak, Chris C. *Wars of Disruption and Resilience*. Athens: The University of Georgia Press, 2011.

Gray, Colin S. *Modern Strategy*. Oxford: Oxford University Press, 1999.

Greenberg, Andy. "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel (Video)." *Forbes*, 24 July 2013. www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 24–42. Washington, DC: Potomac Books, 2009.