A Gender Analysis of Cyber War

A Gender Analysis of Cyber War

Alexandria M. King-Close

A Thesis in the Field of International Relations

for the Master of Liberal Arts in Extension Studies

Harvard University

May 2016

Abstract

This thesis is a gender analysis of cyber war. Cyber war is a relatively recent domain within the context of international conflict. Thus far, neither a gender analysis of cyber warfare, nor of those who carry out cyber warfare—in other words cyber warriors, seems to have yet been conducted. Though existing literature discusses many other aspects of cyber war, it lacks any significant focus on gender analysis or gender perspective, if it mentions gender aspects at all. Furthermore, little analysis seems to have been conducted around cyber warriors themselves. This analysis evaluates existing literature about cyber war, gender and technology, and gender and war; and cyber warriors themselves, including official United States government entities, leadership, and the cyber war workforce; and cyber warriors of other states, with focus on those of Russia and China.

Overall, this gender analysis concludes that the cyber war landscape holds positive potential for evolving into a fairly gender-equal environment. Interestingly, cyber war appears to hold this potential particularly more promisingly than do the kinetic warfare or technology sectors. Previous academic discourse would lead one to believe that cyber war is considerably biased toward hegemonic masculinity. However, significant initiatives in cyber war leadership, particularly by the U.S. military cyber war community, reveal convincing evidence of efforts to improve inclusion among the cyber warrior workforce that hold promising potential for the future of gender and cyber war. Given that the U.S. military is largely considered to be the world leader in the cyber war arena, its leadership in initiating policies moving gender equality *forward*—rather than enabling it to stay static or even fall backward toward digression, holds potential for impacting cyber war cultural shifts worldwide.

Furthermore, several aspects about working in cyber war may counteract some of the barriers that have deterred women and other minority groups from pursuing roles relating to warfare in other domains, and also in technology. Cyber war may not only lend itself to a more diverse workforce than traditional war and technology have tended to attract, but its resulting more diverse workforce holds potential to bring innovative wartime strategic thinking to the forefront, and also to the technology sector. Cyber war has been identified by many as a new wartime domain requiring new ways of thinking about war and technology. Significantly, cyber war may itself bring a fresh perspective to both the technology sector and wartime mindsets, opening new opportunities for innovation and creative problem solving.

Table of Contents

Introduction

This thesis is a gender analysis of cyber war. Cyber war is a relatively recent domain within the context of international conflict.[1] Thus far, neither a gender analysis of cyber warfare, nor of those who carry out cyber warfare—in other words cyber warriors, seems to have yet been conducted. Existing literature about cyber war is relatively robust, particularly given that it is a fairly new aspect of international conflict literature. Though existing literature by and large discusses many other aspects, it lacks any significant focus on gender analysis or gender perspective, if it mentions gender aspects at all. Books and articles about cyber war often discuss characteristics both technical, such as how particular types of cyber attacks are conducted from a very specific technical understanding; as well as conceptual, deliberating the broader picture of the unique aspects of cyber war and cyber attacks and how they interplay with other, more traditional means of warfare and relations between states and other actors.

Cyber war, or *cyber warfare*, is defined by Rand Corporation as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[2] U.S. Secretary of Defense Ashton Carter has described cyberwarfare as "a cyberattack on critical infrastructure, the economy or U.S. military operations."[3] [4] This definition, however, varies some

---

[1] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek Reveron, Kindle edition (Georgetown University Press, 2012), Location 64.

[2] This definition was excerpted directly from: "Cyber Warfare," Rand Corporation, <http://www.rand.org/topics/cyber-warfare.html>.

[3] Bill Gertz, "Carter Defines Acts of Cyber War," February 5, 2015, http://freebeacon.com/national-security/carter-defines-acts-of-cyber-war/.

according to who it is defining the term. According to the United States Cyber Command, which falls under U.S. Strategic Command, *cyber warfare* is defined as "Creation of effects in and through cyberspace in support of a combatant commander's military objectives, to ensure friendly forces freedom of action in cyberspace while denying adversaries these same freedoms. Composed of cyber attack, cyber defense, and cyber exploitation."[5] As most effectively suits the U.S. military's use of the term, the latter definition specifies military contexts of actors such as the combatant commander. For the purpose of this study, the former definition from Rand Corporation will primarily be used, with understanding of other specific definitions relevant to specific groups such as the U.S. military. The definition of *cyber warrior* used will be, a person who conducts cyber war. Although not specifically stated, this understanding of the meaning of cyber warrior is implied as such by several documents and articles from the U.S. Department of Defense.[6] [7] [8]

Although considerable gender analysis has been discussed with regard to technology, and to war, the two fields have not been discussed but minimally where they all three intersect at gender and cyber war. Furthermore, little analysis seems to have been conducted around cyber warriors themselves, or in other words, those individuals and groups who conduct cyber warfare.

---

[4] Bill Gertz, "Ashton Carter Outlines Acts of Cyber War," *The Washington Times*, February 4, 2015, sec. News - Inside the Ring, http://www.washingtontimes.com/news/2015/feb/4/inside-the-ring-ashton-carter-denies-north-korea-c/.

[5] "Cyber Warfare Lexicon - A Language to Support the Development, Testing, Planning, and Employment of Cyber Weapons and Other Modern Warfare Capabilities" (USSTRATCOM, January 5, 2009).

[6] Ibid., 15.

[7] Donna Miles, "Defense.gov News Article: Cyber Command Builds 'Cyber Warrior' Capabilities," September 27, 2011, http://archive.defense.gov/news/newsarticle.aspx?id=65459.

[8] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture | Small Wars Journal," *Small Wars Journal*, July 29, 2010, http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture.

Cyber war is a realm that is particularly difficult to identify who the individual actors behind specific acts are, let alone using those identities to shed light on their intentions and motivations. However, the information that is available about how cyber groups are organized, state cyber strategies, and characteristics both observed about these groups directly as well as indicated based on their actions, illustrate some significant observations in terms of a gender analysis of cyber war and cyber warriors.

Chapter I

Gender Analysis of Cyber War

In conducting a gender analysis of cyber war, firstly existing literature will be examined. This will consist of analyzing terminology related to gender in literature specific to cyber war, a review of literature on the intersection of gender and technology, and a review of literature on the intersection of gender and war.

Analysis of Gender-Related Terminology in Cyber War Literature

To gain an understanding of how gender is discussed in existing cyber war literature, I conducted a series of keyword searches of terms specifically related to gender within a sample of books and other sources about, and specifically relevant to, cyber war.

Methodology

To select the sample of relevant literature, I searched in Harvard University Library's Hollis catalog system, and reviewed the first 50 book entries from a keyword search of "cyber AND war", and a second search of "cyber". All sources related to cyber war were analyzed. Eliminated from the sample were materials whose focus was different than cyber war, such as cyber-bullying; and materials that were not available in digital form, to allow feasibility and accuracy of word counts; and materials in languages other than English. For each of the resulting sources, I performed a keyword search of seven keyword terms that would indicate discussion

about gender, consisting of: *gender*; *masculin**, including masculine, masculinity, and other terms with prefix masculin-; *feminin** including feminine, femininity, and other terms with prefix feminine-; *sex*; *women*; *male*; and *female*. The quote or short passage including each instance of a keyword term was then listed.

Results and Analysis

Nine of the 26 sources, or roughly one third, did not have any mention at all of any of the key gender related terms. The number of instances of each term across the sources are as follows:

Gender Analysis-Related Term Usage in Cyber War Literature	
Term	**Number of instances used**
gender	16
masculin* Includes *masculine*, *masculinity*, and other terms with prefix *masculin-*	Zero
feminin* Includes *feminine*, *femininity*, and other terms with prefix *feminin-*	Zero
sex	19
women	31
male	6
female	4

In analyzing the instances where terms related to gender analysis are used in cyber war literature, the usage falls into several categories. Firstly, several mentions are used to point out the diversity of people involved in cyber space, however those brief mentions do not significantly elaborate on the topic. Some sources even specifically mention that the demographics of those who often interact within areas of the cyber environment are different from the demographics that commonly held stereotypes may lead one to believe may describe the average user. For example, Derek Reveron mentions, "Gone are the stereotypes of young male gamers that dominate cyberspace; those that inhabit the virtual world are increasingly middle-aged, employed, and female."[9] He goes onto explain that about half of users of the virtual program "Second Life," and also Facebook users, are women.[10] However, the short paragraph mentioning this point is the extent to which the author explains it, without elaboration beyond more than brief mention. While a gender analysis would appreciate that a perhaps unexpected demographic population is more active in the cyber arena than a typical observer may at first presume, cyber war literature significantly lacks robust analysis beyond brief mention of this point.

The second category of the use of gender analysis-related terms is in cultural examples of other cultures' use or reference to women as victims or objects for use in war, rather than as significant players themselves in the landscape of war. For example, *Inside Cyber Warfare* mentions, in the context of Chinese military strategy, the tactic of using women as sexual objects

[9] Reveron, *Cyberspace and National Security*, Location 126.

[10] Ibid., Location 128.

to distract adversaries, known as a 'honey pot' strategy.[11] This refers to women as a tool or weapon of war, as *objects* for use in war rather than *subjects* of significant actions themselves.

In these such cultural example usages, what appears to lie in between the lines is implication that other cultures have backward or outdated or rudimentary views of gender in war, contrasting with a lack thereof mentioned in discussion about Western warfare tactics. The irony is that the discussions about Western tactics lack much significant mention at all about gender dynamics in terms of cyber war. This lack of mention could imply that gender dynamics are such a nonissue that Western war culture has advanced past them and therefore they are not worth mentioning. However, the extent of this *lack* of addressing existing dynamics strongly risks overlooking significant not only *overt,* but perhaps more importantly, *underlying* gender-related dynamics at play.

The third usage of gender analysis-related terminology is historical examples of social norms and movements, used in vague parallel comparison to a historical analysis and long-term perspective of cyber war. This includes reference to movements such as the women's suffrage movement, the social movement advocating opposition to violence against women, and so forth. Although a gender analysis would appreciate these nods to the impact of gender-related and feminist movements, brief mention of them as examples against myriad other historical movements is unlikely to influence broader gender perspective thinking within discussions about cyber war.

The fourth usage of gender terminology is direct quotes from historical figures relating to warfare. This usage particularly mentions 'women and children' and equivalent terms that seem to emphasize outdated notions of overgeneralization; sexism; and victimization of women by

[11] Jeffrey Carr, *Inside Cyber Warfare*, 1st ed. (Sebastopol, Calif: O'Reilly Media, 2010).

their being only referred to within the context of those groups. For example, Brian Mazanec refers to Adolf Hitler and Neville Chamberlain in the context of World War II:

> National leadership did seem to declare support for the norm on the eve of conflict, with Hitler announcing that he would restrict Luftwaffe bombing to military targets and Prime Minister Neville Chamberlain declaring that Britain would 'never resort to the deliberate attack on women and children, and other civilians for the purpose of mere terrorism.[12]

However, these types of references tend not to analyze what exactly has changed, in terms of how societal understandings of war, or political leaders' emphases, have grown more sophisticated to reflect the more complex realities of such groups.

A related observation worth mentioning is that the phrase "women and children" is used many times in multiple publications, and constitutes a large number of the instances of the word 'women' in cyber war literature. One quarter of the instances when the term "women" is used, it is used specifically in the phrase "women and children," without the word 'women' being used separately from 'children.' The phrase is used about 25%, eight times of the 31 total uses of the term 'women.' The use of *women and children* considered together indicates women as an objectified minority group,[13] diminishing their agency as adult actors, and instead of allowing them to be subjects who act, limiting them to being objects about which *others* talk, and on behalf of whom *others* act.

Furthermore, the phrase *women and children* is used as an example of noncombatants, grouping women together with children, assuming that both groups—both separately and combined—are noncombatants. One example of this is in the quote from Mazanec's *The*

---

[12] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (U of Nebraska Press, 2015), 93.

[13] Ann Oakley, "Women and Children First and Last: Parallels and Differences between Children's and Women's Studies," in *Children's Childhoods: Observed And Experienced*, ed. Berry Mayall (Routledge, 2002), 14.

Evolution of Cyberwar: "Rather, what was compelling was the idea of this new, yet to be invented super poison weapon—modern CW—that could be used 'against towns for the destruction of vast numbers of noncombatants, including women and children.'"[14] Even within a quote from another source, by not addressing the bias of using the term broadly categorizing women with children in such a way, this term usage, and by extension the objectification of women as a noncombatant group, accepts and even endorses only mentioning women within this limited context.

The fifth category of instances of gender-related terminology refers to anecdotes about specific people involved in cyber war. These mention individuals' involvement in sexual crimes, or instances in their own personal histories where mention of these involvements in sexual crime, or their own identities, seem to be used to characterize, or contextualize them as characters in the narrative stories about cyber war. For example, in the book *Cybersecurity and Cyberwar: What Everyone Needs to Know,* P. W. Singer and Allan Friedman refer to sexual assault allegations of Julian Assange, in the context of describing his involvement in a leak of classified information.[15]

Mentioning sexual assault in specific cases in such a way seems to be trying to demonstrate character, personal background, or the social situational context of events relating to specific cyber security situations. The authors later mention individual gender identity in discussion about Bradley Manning, a U.S. Army private who was accused of publishing classified military documents, mentioning his gender identity disorder.[16] This note about Manning seems to be used to provide background to his broader narrative. In both of these and

[14] Mazanec, *The Evolution of Cyber War*, 45.

[15] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Kindle edition (Oxford University Press, 2013), Location 1048.

[16] Ibid., Location 4987.

other instances of using gender-related terms about specific people involved in cyber war, these observations or characteristics are used as part of the authors' depiction of the story about specific information leaks or other cyber security related occurrences. Instances in the literature mentioning these aspects of particular individuals is rather brief, and authors do not overtly expand upon why such gender-related observations or characteristics are included in descriptions about particular individuals. However, the fact that they do include these specific characteristics or activities does indicate the authors' perception that gender-related aspects of one's identity or past experiences are relevant to the conversation about cyber war, at least on a personal level.

The sixth category of gender-related terminology use is in legal protections against things like discrimination. In *Cyber-Attacks and the Exploitable Imperfection of International Law*, Yaroslav Ridiziwil refers to international law documents Draft Convention for the Protection of Civilian Populations Against New Engines of War, and the United Nations General Assembly Resolution on the Declaration on the Protection of Women and Children in Emergency and Armed Conflict.[17] In these cases, the terms are not elaborated on, rather only used within the references to and titles of specific legal doctrines. Like many other categories of gender-related terminology use in cyber war literature, this too indicates that authors seem to acknowledge on some level that gender-related aspects are relevant to conversations of cyber war, but only mention it on the peripheries without much, if any, explanation.

The seventh type of gender-related terminology usage talks about gender or sex as a type of personally identifiable information, which 1) may become vulnerable in terms of cyber security, and 2) can be manipulated to construct a virtual identity that may differ from one's real-world identity. As far as gender and sex being personally identifiable information about people

---

[17] Yaroslav [author Radziwill, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Leiden ; Boston: Brill Nijhoff, 2015, 2015), 191.

that can be vulnerable to being hacked into or revealed by others, mention of this in cyber war literature is often not emphasized but itemized within larger lists of other information, such as along with birth dates and phone numbers. For example, in Jeff Shantz's discussion about Sony Entertainment being hacked in 2011, he mentions gender as one type of personal information that hackers obtained, alongside mentioning credit card numbers, email addresses, passwords, and birth dates.[18] What this says about gender in the cyber arena, is that these personal descriptors are meaningful information that people value and also that they consider private, or at least that they view it a violation of personal privacy when others reveal that information about them without their own permission or knowledge. Although brief mentions of gender within longer lists of demographic descriptors do not overtly say so, their presence in these contexts indicates the value and also the personal nature of gender as a type of significant information about people in the cyber arena.

The ability to manipulate one's perceived gender online brings to light additional discussion points. Gender being one, among a myriad of aspects of personal identity that can be so easily manipulated in the cyber environment, begs the question: is gender even relevant to analyze in the cyber context? From a perspective of gender studies, the existence of the discipline itself, as well as the wide scope of arenas in which theorists employ a gender perspective,[19] implies that gender impacts aspects of society and individuals' lives in ways even beyond what may be consciously recognized. Furthermore, research in several disciplines has discussed other arenas in people's lives showing that gender does indeed impact how people

---

[18] Jeff [author Shantz, *Cyber Disobedience : Re://presenting Online Anarchy* (Winchester, UK ; Washington, USA: Zero Books, 2014).

[19] Kristin Switala, "The Feminist Theory Website: English Introduction," accessed February 8, 2016, http://www.cddc.vt.edu/feminism/enin.html.

view and are viewed. For example, scientific sex differences have been shown to make a difference for girls and boys, and women and men in the classroom,[20] [21] and biological as well as social differences between women and men also impact people's health.[22] [23] Thus, although at first glance it may seem that the manipulability of gender identity suggests that gender is not a particularly relevant identity lens worth analyzing in the context of cyber war, the fact that it is relevant that it can be and is manipulated, and that such identity manipulation does indeed play a meaningful role in cyber activities, attests that gender is relevant after all.

Of the multitude of materials analyzed here, one particular mention of a gender perspective substantively discusses gender issues within the context of cyber war. Interestingly, it is found in a book focusing on cyber terrorism, rather than cyber war or cyber attacks, per se. In his book *Cyber Terrorism : Political and Economic Implications*, Andrew Colarik discusses that some terrorist groups perceive women "as agents of social change, and [seek] to moderate or eliminate their capacity to institute change through violent intimidation. Freedom of thought and self-expression is not the only action terrorists seek to control through intimidation."[24] Here, women are a specifically identified group that is viewed, in this case by certain terrorist groups, as having a unique potential to instigate social change. In this case, the motivations of the

---

[20] Leonard Sax, *Why Gender Matters: What Parents and Teachers Need to Know about the Emerging Science of Sex Differences* (Potter/TenSpeed/Harmony, 2007).

[21] Susan A. Basow, "Student Evaluations of College Professors: When Gender Matters," *Journal of Educational Psychology* 87, no. 4 (1995): 656–65, doi:10.1037/0022-0663.87.4.656.

[22] Chloe E. Bird and Patricia P. Rieker, "Gender Matters: An Integrated Model for Understanding Men's and Women's Health," *Social Science & Medicine* 48, no. 6 (March 1999): 745–55, doi:10.1016/S0277-9536(98)00402-X.

[23] Debra L. Roter and Judith A. Hall, "Why Physician Gender Matters in Shaping the Physician-Patient Relationship," *Journal of Women's Health* 7, no. 9 (November 1, 1998): 1093–97, doi:10.1089/jwh.1998.7.1093.

[24] Andrew M. Colarik, *Cyber Terrorism : Political and Economic Implications* (Hershey, PA: Idea Group Pub, 2006), 19.

adversary—i.e. terrorists, are observed to perceive women to be uniquely positioned tending toward certain capabilities, and thus that women pose a unique threat to terrorists' ambitions.

Given that this is the only found substantive discussion about a gender perspective that has been identified in this analysis of cyber war literature, begs the question, why are gender-related motivations of adversaries *not* mentioned in relation to cyber war adversaries other than terrorist groups? For example, might state actors view particular demographic groups as posing unique threats to their state cyber war capability, and thus strategize differently against certain adversary demographic groups than others? In better understanding the motivations of cyber war actors, it is worth considering whether and how cyber war actors such as states might view certain demographic groups as posing unique threats in the cyber arena. Perhaps the analysis of cyber war in general is too new and too misunderstood terrain at this point for scholars to grasp whether this might be worth exploring further.

In conclusion, this method of keyword searches of gender-related terms in existing cyber war literature is certainly not a perfect technique for analyzing discussion about gender in existing literature. There are obviously ways to meaningfully discuss gender aspects of cyber war without actually directly using any of the keyword terms for which this method searched. However, this keyword term search does provide a reasonable snapshot of the extent to which gender aspects are discussed in cyber war.

Overall, existing cyber war literature discusses gender in only very limited ways. Most instances of gender-related terminology are within contexts of brief mentions, many within lists of multiple axes of demographic categories, and in many cases within authors' efforts to tell narrative stories about cyber security situations perhaps to give them creative color or make them more interesting to the reader. Though the instances where gender is mentioned are brief, their

existence and often the broader contexts of meaning within which they lie, do indicate that scholars and other experts who have written about cyber war have recognized the significance of gender aspects to some degree. That said, considerable additional work is yet to be done if gender aspects are to truly be addressed within the broader discussion of cyber war.

Review of Existing Literature on Gender and Technology, and Gender and War

Although there is little mention in existing literature about gender aspects of cyber war, the closest relevant material that does provide a gender analysis, is that of gender and technology, and gender and traditional war. Overall, literature about gender and technology emphasizes connections between technology and masculinity, with masculinity being the hegemon, and women adapting in various ways to it. Gender and war literature overarchingly emphasizes how war is considered masculine as well.

Gender and Technology

Sherry Turkle's work provides a key basis from a sociological perspective of how people view and view their use of technology, including analysis from gender perspective. Her earlier work in the late 1980's and early 1990's included analysis of gender dynamics in relation to using technology. In the article "Computational reticence: Why women fear the intimate machine," she discusses how women tend to feel less comfortable with technology such as hacking, because it threatens them by having human characteristics that they perceive they are supposed to have, according to society. However, men view technology differently. Turkle emphasizes ways how people perceive technology as lending itself more so to men than women

— or in other words, more aligned with masculine than feminine characteristics.[25] Through this lens of analysis, cyber war, given its position as a field intimately embedded in technology use, would be assumed and perceived to also lend itself more easily to men than to women. However, perceptions about gender and technology use may well have evolved in significant ways between the 1980's and 1990's when Turkle published these works and 2016 at the time of writing, which may impact change in how people perceive men's and women's use of, and comfort in using technology.

Though some of her earlier works discuss women and technology, Turkle's more recent works in the later 2000's discuss technology in everyday life without considerable focus on differences relating to gender. Perhaps as technology such as smart phones, tablets, the Internet of Things, etc., are becoming more pervasive in our lives, technology is becoming less divided between men and women in terms of perceptions of comfort and accessibility. To put it simply, maybe women are less fearful of technology in 2016 than they were as Turkle described back in 1988.

In her more recent work in the 2010's, Turkle observes how ways of interacting with one another through digital communications is affecting people's tendencies of how they communicate. Notably, with the prevalence of email, instant messaging, the 140-character-limited Twitter, and so forth, people are tending to communicate in smaller amounts of information that they give and expect to receive more immediately.[26] [27] These communication tendencies in the 2000's and 2010's are not specified to differ between women and men, but

[25] Sherry Turkle and Cheris Kramarae, ed., "Computational Reticence: Why Women Fear the Intimate Machine," in *Technology and Women's Voices: Keeping in Touch* (Routledge, 1988), 33–49.

[26] Sherry Turkle, "The Flight From Conversation," *The New York Times*, April 21, 2012, http://www.nytimes.com/2012/04/22/opinion/sunday/the-flight-from-conversation.html.

[27] Megan Garber, "Saving the Lost Art of Conversation," *The Atlantic*, February 2014, http://www.theatlantic.com/magazine/archive/2014/01/the-eavesdropper/355727/.

rather are an overarching cultural and societal trend spanning across demographics throughout Western society and across the world. This tendency is inhibiting people's ability to discuss and even process complex ideas, on a societal level.[28] [29]

What, then, does this mean in terms of cyber war? On one hand, overall trends in communication between people may be assumed to be essentially the same regardless of sector, meaning that its effect in cyber war would be unremarkable in comparison to virtually any other sphere. However, the fact that cyber war by its nature can only take place within the cyber domain, elsewise it would not be considered cyber war as such, suggests that technologically related communication tendencies would be more likely to have a stronger effect in cyber war than it might in fields such as, say, traditional or kinetic war.

A variety of other feminist scholars have analyzed a feminist perspective in relation to cyber space and technology. The concept of cyberfeminism[30] is one key analysis at the intersection of gender and the cyber arena. Among the theories within the discourse on cyberfeminism are that technology has been considered 'masculine' by some feminists.

If technology is considered to be masculine, from a gender analysis perspective, likely cyber war would also be considered to fall readily within what is viewed as masculinity. This would certainly impact not only how cyber war is viewed broadly, but also how cyber warriors would be likely to view themselves in terms of their position within a gendered dichotomy. Furthermore, cyber war being considered 'masculine' would impact how strategists use cyber war, given that war strategies vary in terms of how much strength they are perceived to

---

[28] Turkle, "The Flight From Conversation."

[29] Garber, "Saving the Lost Art of Conversation."

[30] Mia Consalvo, "Cyberfeminism," *Encyclopedia of New Media* (Thousand Oaks, CA: Sage Reference, 2002), http://study.sagepub.com/sites/default/files/Ch17_Cyberfeminism.pdf.

indicate.[31] As Carol Cohn observes, gender-driven rhetorical concepts such as 'acting like a wimp' in discussions about wartime strategic decisions indeed can and do affect the strategic decisions that leaders make, as well as what goes into how they make those decisions.[32] Ultimately, the perceived masculinity of the field of war itself, and perhaps of technology as well, shape how specific strategies and actions within those domains are valued. In turn, gendered perceptions valuing some strategies and actions above others affects decision making processes along with how eventual outcomes are valued.

Other feminist perspectives hold perhaps more optimistic views in terms of women's relationship with technology. Sadie Plant, for example, has argued that cyber and related technologies lend themselves well for women to adopt, making it easier to realize characteristics seen as women's strengths such as connecting with people.[33] Similarly, other related literature discusses how the cyber arena allows women more freedom from the barriers of gender than the real world, such as Judy Wajcman, who argues that women's use of technology equalizes the playing field, so to speak.[34]

These gender analysis perspectives can well be considered relevant in cyber war as well. If cyber technology skills are comparatively easy for women to assume, cyber may be a domain in the war scape where women are more readily welcomed than, for example, in traditional combat roles. If this is the case, their ease in involvement in cyber war may likely affect how

---

[31] Carol Cohn, Miriam ed. Cooke, and Angela ed. Woollacott, "Wars, Wimps, and Women: Talking Gender and Thinking War.pdf," in *Gendering War Talk* (Princeton, New Jersey: Princeton University Press, 1993), 227–46.

[32] Ibid., 234–235.

[33] Consalvo, "Cyberfeminism."

[34] Judy Wajcman, "Technocapitalism Meets Technofeminism: Women and Technology in a Wireless World," *Labour & Industry* 16, no. 3 (May 2006): 7.

cyber warriors conduct cyber war, and perhaps even how strategic decisions in this arena are made and executed.

Many viewpoints in feminist work include discussion about why women should become more proficient in cyber skills.[35] One such perspective is that of Donna Haraway, who confers that not only should women become more proficient in using new technologies, but furthermore, they should view their technology use as a way to challenge larger systems that marginalize them.[36] This perspective can certainly be relevant in a gender analysis of cyber war as well. Women growing more comfortable with using and conceptualizing cyber war technologies could level the playing field in the war landscape in terms of gender in new ways. Where kinetic war has traditionally been considered biased toward valuing men and masculinity,[37] [38] women's increased involvement in cyber warfare could lend cyber war to new heights in terms of bringing increased gender equality to the conflict arena overall.

Beyond analyzing feminism and femininity relating to technology, there is also some literature examining masculinity and cyber space. Several observations show contradicting associations of masculinity and technology. Melodie Calvert and Jennifer Terry compile views about relations between technology and notions of gender including masculinity, describing desire for technology even in sexual or pseudo-sexual terms, and also a fear of technology.[39]

---

[35] Donna Haraway, "A Cyborg Manifesto: Science, Technolgy, and Socialist Feminism in the Late Twentieth Century," in *Simians, Cyborgs and Women: The Reinvention of Nature* (New York: Routledge, 1991), 149–181.

[36] Ibid.

[37] Leo Braudy, *From Chivalry to Terrorism: War and the Changing Nature of Masculinity*, Kindle Edition (Vintage, 2010).

[38] Paul Kirby and Marsha Henry, "Rethinking Masculinity and Practices of Violence in Conflict Settings," *International Feminist Journal of Politics* 14, no. 4 (December 2012): 445–49, doi:10.1080/14616742.2012.726091.

[39] Jennifer Terry, ed. and Melodie Calvert, ed., *Processed Lives: Gender and Technology in Everyday Life* (Psychology Press, 1997).

These perspectives may make becoming a cyber warrior uniquely appealing, or particularly uninviting, respectively.

Éva Zékány analyzes masculinity and geek identity, showing the dynamism of masculinities including historical and pop culture examples.[40] Other studies examining about how masculinity is portrayed in popular culture show opposing portrayals, such as the male subject being feminized, but also hyper-masculinized.[41] Existing literature discusses that masculinity relating to cyber space is distinct from other expressions of masculinity. Furthermore, popular culture such as science fiction books and films show cyber space and users of technology in gendered ways. Perhaps these considerably varied conceptions of gender and technology could allow more nuanced views about cyber war in terms of gender, than gendered perceptions of traditional war may have acknowledged.

In summary, existing literature around gender and technology discusses ways that the rise in prevalence of digital communications affects societal-level communication and capability and motivation to discuss complex ideas; and that cyber technology is viewed in gendered ways, not only differently in terms of femininity but particularly complex and varied in relation to perceptions of masculinity. However, there is a relationship connecting gendered perceptions of activity in the cyber environment, capability and tendencies of *how* people communicate, and perceptions of the threat of cyber war. Although many scholars and feminists view technology as being masculine, it is also valuable to compare masculinity in terms of cyber war, versus

---

[40] Eva Zekany, "The Gendered Geek: Performing Masculinities in Cyberspace" (Central European University, Department of Gender Studies, 2011).

[41] Amanda Fernbach, "The Fetishization of Masculinity in Science Fiction: The Cyborg and the Console Cowboy," *Science Fiction Studies* 27, no. 2 (July 2000): 234–255.

masculinity in terms of kinetic war. The intersection of these arguments and perceptions affect perceptions of the threat of cyber war, and furthermore, capabilities to prepare for cyber war.

Gender and War

In the Encyclopedia of Sex and Gender, the entry on Gender and War states, "The gendered character of warfare is extraordinarily consistent across human cultures." [42] The literature analyzing gender in the realm of traditional war is rather immense, and spans several academic disciplines, including sociology, gender and women's studies, anthropology, political science, and international relations, among others. That said, in the long view, historians have not viewed feminism or a gender perspective as a relevant lens through which to analyze war and diplomacy.[43]

Though broad and varied, many of the gender and war discussions involve significant discourse on: 1) How war initiates shifts in social fabric such as traditional gender roles; 2) Gendered aspects—and the meanings around them—of sexual violence used as a weapon of war; 3) women's roles in war, including in support roles, as combatants (though they tend to be in the minority when combatants), in other community leadership roles particularly broadening beyond their non-wartime roles, and as victims and harborers of peace—including critique of overemphasizing their roles as victims and pacifists; and 4) what war reveals or how it shapes understandings and personifications of masculinities.

---

[42] Joshua S. Goldstein, "War and Gender," in *Encyclopedia of Sex and Gender*, ed. Carol R. Ember and Melvin Ember (Springer US, 2003), 107, http://link.springer.com.ezp-prod1.hul.harvard.edu/referenceworkentry/10.1007/0-387-29907-6_11.

[43] Joan W. Scott, "Gender: A Useful Category of Historical Analysis," *The American Historical Review* 91, no. 5 (December 1986): 1057.

Traditionally, and extending to present-day trends, those who fight in war tend to be largely male.[44] Given the changing roles, including physical movement, of men during wartime, opportunities for women to take up roles that would otherwise have been held by men is a common type of gender role shift that occurs during times of war.[45] Although women, as well as other groups, often undertake functions during wartime that they unlikely would otherwise, such new dynamisms in their roles often do not last long after war ends, though in some cases new roles continue afterward.[46] [47]

Men's roles are also discussed considerably, particularly in terms of changing concepts and embodiments of masculinity. As Leo Braudy observes, "War is the ultimate landscape for demonstrating or proving masculinity, across a multitude of societies and cultures…this war system is among the most consistently gendered of human activities." [48]Times of war often present occasions for men to prove their masculinity, through ways including physical capability, violence, dominating others, and representing heroism.[49]

Cyber war is a rather different environment in terms of these aspects of gender and traditional war. Where in traditional war, soldiers must physically and geographically leave their homes and communities to fight, cyber warriors need not necessarily leave their communities or even their own homes to fight cyber war. While this may mean that activities initiating gender

---

[44] Goldstein, "War and Gender," 107.

[45] Penny Summerfield, "Gender and War in the Twentieth Century," *The International History Review* 19, no. 1 (March 1997): 6–7, doi:10.1080/07075332.1997.9640771.

[46] Mary H. Moran, "Gender, Militarism, and Peace-Building: Projects of the Postconflict Moment," *Annual Review of Anthropology* 39, no. 1 (October 21, 2010): 261–74, doi:10.1146/annurev-anthro-091908-164406.

[47] Rivka Weiss Bar-Yosef and Dorit Padan-Eisenstark, "Role System Under Stress: Sex-Roles in War," *Social Problems* 25, no. 2 (December 1, 1977): 135–45, doi:10.2307/800290.

[48] Braudy, *From Chivalry to Terrorism*, Location 180.

[49] Braudy, *From Chivalry to Terrorism*.

norm shifts may not be common in cyber war in some ways, it may present gender norm shifts in ways that traditional war may not. For example, someone who wants to contribute to an interstate conflict but is not willing or able to leave their community or family in order to do so, could potentially serve as a cyber warrior while geographically not leaving their own community. Flexibility in geographical location of cyber warriors offers a job role flexibility in ways that traditional combatants have not often had.

Cyber war may also indicate masculinities in ways that may be parallel to, and may be different from, traditional war. Cyber warriors' self-identities and views of themselves may reflect those of traditional warriors, which are seen as traditionally masculine such as being physically strong and heroic, while perhaps concurrently reflecting identities of computer savvy hackers, or 'geeks.' As Éva Zékány discusses, what she deems 'geek masculinity' is complex and multifaceted, oriented as being non-femininity.[50] In similar ways, warrior identity is multifaceted and defines itself in contrast to its opposite, femininity.[51] Cyber warriors' views of themselves and their incarnation of gender identity would likely consist of a combination or intersection of traditional warrior identity, and geek identity.

In summary, there is a fairly robust collection of gender analysis research and reflection in terms of technology, and in terms of war. However, a gender analysis of cyber war has not yet been analyzed to any length comparable whatsoever to existing dialogue of gender analysis in terms of technology or war. Nonetheless, the gender analysis lens used to examine technology and war provide a considerably useful framework in conducting a gender analysis of cyber war.

[50] Zekany, "The Gendered Geek: Performing Masculinities in Cyberspace."

[51] Braudy, *From Chivalry to Terrorism*.

Chapter II

Gender Analysis of Cyber Warriors

In analyzing cyber warriors from a gender perspective, firstly those who practice cyber war will be identified and discussed. Secondly, official government entities that are considered cyber warriors will be analyzed, beginning with cyber war leadership in the United States government, and then the cyber war workforce within the United States government. Cyber warriors of states other than the United States will be analyzed next, with particular focus on Russian cyber warriors, and Chinese cyber warriors.

Who Practices Cyber War

In terms of analyzing who it is who practices cyber war, there are several groups that can be considered. Firstly, the definition of what constitutes a cyber warrior is necessary to discuss. A cyber warrior is generally considered a person who conducts cyber war. Although this definition is not explicitly stated, it is often implied in discussion about cyber war.[52] [53] [54] [55] [56] [57][58]

---

[52] "Cyber Warfare Lexicon - A Language to Support the Development, Testing, Planning, and Employment of Cyber Weapons and Other Modern Warfare Capabilities," 15.

[53] Miles, "Defense.gov News Article: Cyber Command Builds 'Cyber Warrior' Capabilities."

[54] Robert Hackett, "Gasp! China Admits to Having Cyber Warriors," *Fortune*, March 26, 2015, http://fortune.com/2015/03/26/china-admits-cyber-warriors/.

[55] "Internal DoD Effort Focuses on Individual Cybersecurity Responsibility > U.S. DEPARTMENT OF DEFENSE > Article View," October 14, 2015, http://www.defense.gov/News-Article-View/Article/622987/internal-dod-effort-focuses-on-individual-cybersecurity-responsibility.

[56] Conti and Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture | Small Wars Journal."

Although non-state actors have increasingly been found to conduct significant cyber attacks in recent years,[59] state actors and those who conduct acts of cyber war on behalf of states, remain the key set of cyber warriors when considering cyber war to consist of cyber attacks primarily among states.

Terminology of what to call cyber warfare and those who are experts in is very much still in the midst of debate. At the time of writing, head of U.S. Navy Fleet Cyber Command Vice Admiral Jan Tighe is currently conducting a survey from navy Information Warriors about how most aptly to rename 'information warfare,' suggesting a new name and branding as 'Cryptologic Warfare'.[60] If the term *cryptologic warfare* is ultimately adopted, and indeed whatever term is decided upon, the Navy will be positioned to define its meaning,[61] which will further shape cyber war culture within the U.S. military and particularly among cyber warriors themselves. This shift may also alter the gendered dynamics of the cyber war arena, in ways that remain to be seen.

Within conversations among academics and technical experts about cyber war, one aspect that emerges often is that of defense versus offense.[62] In the realm of cyber war, offensive and

---

[57] United States Department of Defense, *The Making of a Cyber Warrior - DoD News*, Youtube Video, 2013, https://www.youtube.com/watch?v=WbmTqzLHBGA.

[58] Dune Lawrence, "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016," *BloombergView*, April 15, 2014, http://www.bloomberg.com/bw/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete.

[59] Laurie R. Blank, "International Law and Cyber Threats from Non-State Actors," *International Law Studies, U.S. Naval War College* 89, no. 406 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2194180.

[60] Jan Tighe, "Vice Admiral Tighe's Letter to the Information Warrior Community.pdf," February 12, 2016, http://www.public.navy.mil/fcc-c10f/Pages/home.aspx.

[61] Ibid.

[62] Richard A. Andres and ed. Derek S. Reveron, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Kindle edition (Georgetown University Press, 2012), Location 1936–2321.

defensive activities can be especially difficult to differentiate from one another, due to the technical nature of cyber activities.[63] However, there is a reasonable level of differentiation between those whose focus is mainly on defending one's own cyber entities, versus those whose focus is mainly on offensively attacking an opponent through cyber warfare.[64] Who, then, falls within the potential groups of defensive cyber warriors, and offensive cyber warriors?

At its widest consideration, defensive cyber warriors could entail an enormous group of people, including essentially anyone who intends to stop potential cyber attacks conducted against a state. This could include the cyber security workforce employed within the government, as well as those who work for private sector companies on contracts and through other indirect ways for the government. It may even extend to cyber security employees in the private sector, who work to defend private sector entities, in cases where cyber warriors sponsored by adversary states might attack other states' private sector companies, which often occurs in cases of Chinese cyber attacks on U.S. private companies.[65] A wide definition could also include cyber warriors from private companies for these reasons. Although governments are far from the *only* actors that sponsor cyber attacks,[66] they remain a key relevant set of actors sponsoring cyber warriors' attacks.[67] While an entirely thorough analysis of cyber war would

---

[63] Derek Reveron, "Cyberspace and International Security Class - Government E-1743" (Harvard University Extension School, February 14, 2015).

[64] The Economist, *Richard A. Clarke: Cyberwar in 2013*, Video Interview, 2012, https://www.youtube.com/watch?v=6_ek8mugOUc.

[65] Ibid.

[66] "015 Internet Security Threat Report, Volume 20 - 21347932_GA-Internet-Security-Threat-Report-Volume-20-2015-social_v2.pdf," 69, accessed January 31, 2016, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

[67] John A. Serabian Jr., "Cyber Threats and the US Economy" (Central Intellligence Agency, February 23, 2000), News & Information, Speeches & Testimony Archive 2000, https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

strive to include all entities as may be deemed relevant, due to the limitations of this analysis, cyber warriors included in this study will consist primarily of those who conduct cyber war offensively on behalf of a state.

Given that cyber warfare is a relatively new field within the domains of security and warfare, and that cyber is a particularly quickly changing domain,[68] the undertaking of determining who cyber warriors are is somewhat of a moving target. For example, President Barack Obama announced in February 2015 the establishment of a new Cyber Threat Intelligence Integration Center, under the Director of National Intelligence, which would be a significant initiative in organizing and serving as a hub within the United States government for cyber security threats.[69] However, President Obama outlined that the Cyber Threat Intelligence Integration Center would be fully operational by the end of fiscal year 2016,[70] and at the time of this writing, its official website did not include any information other than the Center's name and two page titles.[71] Furthermore, determining attribution – in other words, who it is who conducted a cyber war attack – is often unclear and even impossible.[72]

In terms of compiling the available information about cyber warriors, there is no single source to date that has comprehensively compiled groups of those who could be considered

---

[68] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Kindle edition (HarperCollins e-books, 2010), Location 530.

[69] "Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center," *Whitehouse.gov*, February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

[70] Ibid.

[71] "404 - Error: 404," accessed January 24, 2016, http://www.dni.gov/index.php/about/organization/ctiic-what-we-do.

[72] Richard B. Andres, "The Emerging Struccture of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, Kindle Edition (Washington, DC: Georgetown University Press, 2012), Location 1972.

cyber warriors. As a result, this analysis requires compiling the various groups, and conducting a gender analysis of them in turn. In broad strokes, cyber warriors consist of two groups: 1) official government entities, including the cyber security workforce that is employed by state governments, and 2) unofficial entities conducting cyber war on behalf of state governments, such as contractors and others who indirectly conduct cyber attacks for states. Although there is considerable ambiguity about the identities and affiliations of cyber warriors in many cases, making it difficult to identify who these two groups consist of by tracing backwards from the attacks they conduct, [73] there is some data that may provide indication about attack origins.

Analysis of Official Government Entities of Cyber Warriors

Official United States government entities that are considered to be involved in the U.S. Federal Cybersecurity Operations Team are the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Department of Defense (DoD).[74] Although the Department of Justice and Federal Bureau of Investigation are relevant actors in the nation's federal cybersecurity realm, their roles pertain largely to cyber crime, and their jurisdiction lies domestically within the United States,[75] which for the most part differs from that of cyber war. While their roles would involve them in attacks within the U.S. that could include involvement in defending against cyber war conducted against the U.S. by another state, this would mainly apply to domestic cyber attacks rather than interstate cyber attacks and

---

[73] Ibid.

[74] "U.S. Federal Cybersecurity Operations Team: National Roles and Responsibilities," March 5, 2013, http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/2013march21_cyberroleschart.authcheckdam.pdf.

[75] Ibid.

warfare. Thus, for the purpose of identifying actors in cyber war, DoJ and FBI are not considered key cyber warrior actors.

Cyber War Leadership in the U.S. Government

In terms of official government entities of cyber warriors, the first specific group to consider is those in leadership positions who would make critical decisions and determine policies about cyber war. This includes high level political leaders, as well as deputy-level leadership. In the United States, the President, as commander-in-chief of the country's military, serves as the ultimate decision maker in terms of cyber war. [76] [77] [78] Deputy-level leadership in the U.S. consists of a combination of political leaders, such as appointees or those whose positions require congressional approval, namely the Secretaries of Defense and Homeland Security; and more technical or operational leaders, namely the head of National Security Administration and U.S. Cyber Command under U.S. Strategic Command. Under US Cyber Command lie the heads of the military service elements, including the U.S. Fleet Cyber Command in the Navy,[79] Army Cyber Command, Air Force Cyber Command, and Marine Forces Cyber Command.[80]

Although some gender analysis can be determined based on the individual leaders' backgrounds and demographics, the key trend worth noting is that most all of their positions,

[76] Michael Sulmeyer, "Study Group: Problem Solving in Cyberspace Operations" (Harvard University Kennedy School of Government, February 2016).

[77] Reveron, "Cyberspace and International Security Class - Government E-1743."

[78] "Thesis on Cyber War - Seeking Advice on Resources," January 2016, https://mail.google.com/mail/u/0/#search/reveron/15236ade57b2e196.

[79] Ibid.

[80] "U.S. Cyber Command - U.S. Strategic Command," accessed January 17, 2016, https://www.stratcom.mil/factsheets/2/Cyber_Command/.

with the exceptions of the Secretary of Homeland Security and the aspects of the President's role beyond commander-in-chief, are oriented within the military. Thus, decisions made in terms of cyber war are made, for the most part, within the context and culture of the military. While it is intuitive that decisions about traditional or kinetic war have historically been made within the military, this militarized orientation becomes a bit fuzzier in terms of cyber war, because unlike in the traditional war landscape, most activity in the cyber arena is conducted by civilians and with civilian intentions. Juxtaposing a military lens to a sphere as civilian-focused as cyber space raises questions about the push and pull between the government military retaining security for its people on one hand, and freedom of speech and activity of citizens in a democratic society on the other.

One of the key elements of a democracy is that citizens are able to engage each other in meaningful dialogue in politics and civic life.[81] From a feminist perspective, such democratic participation should aim to be inclusive of citizens with all gender identities, allowing equal voice to all participants. Cyberspace has uniquely come to provide a sphere in which citizenry can conduct such meaningful democratic dialogue in ways that allow perhaps further equality than has been available in the past, freeing marginalized groups from limitations to which other spheres have often constricted them. The ability to remain anonymous while voicing one's opinions on the Internet to some degree erases others' prejudgments about the person whose opinions they are hearing. Although the military retaining leadership around cyber war makes sense from the perspective of its ability to protect its state's citizenry, this leadership must toe the line delicately to ensure that its security measures do not unnecessarily inhibit the free flow of idea exchange in the cyber sphere.

---

[81] Larry Diamond, "What Is Democracy?" (Hilla University for Humanistic Studies, January 21, 2004), http://web.stanford.edu/~ldiamond/iraq/WhaIsDemocracy012004.htm.

Thus far, there are some significant indications that military leaders are incorporating an effort to shape a fairly inclusive environment in the cyber war arena in terms of gender. One indication is in terminology, in a current initiative lead by Vice Admiral Jan Tighe, who serves as Commander of the U.S. Fleet Cyber Command and Commander of the 10th Command in the U.S. Navy. Vice Admiral Tighe initiated a survey among navy 'Information Warrior' personnel, seeking feedback and ideas for changing the terminology of what the essentially cyber war sector within the navy will call itself and its personnel moving forward.[82] Information warriors are encouraged widely to complete the survey to contribute their feedback, and are offered several avenues through which to access it.[83] [84]

This effort is significant for several reasons. Firstly, high level leadership requesting input from a multitude of levels beneath their position in the chain of command signifies a change in organizational approach from the traditional top-down direction for which the military is known.[85] [86] This may reflect a recognition of cyber war as necessitating new approaches than traditional organizational structure oriented toward kinetic warfare may have. It also reflects other efforts in the more recent 2000's to foster an environment with more equal voice among ranks beyond traditional top-down orientation.[87] Interestingly, Vice Admiral Tighe is the only female among key U.S. cyber war leadership, which may indicate that further diversity among

[82] Tighe, "Vice Admiral Tighe's Letter to the Information Warrior Community.pdf."

[83] Ibid.

[84] "Information Warfare Designator Name Change Survey," Survey, (February 12, 2016), https://www.surveymonkey.com/r/F35YRJ9.

[85] Murray Williamson, "Military Culture Does Matter" (Foreign Policy Research Institute, June 2012), http://www.fpri.org/article/2012/06/military-culture-does-matter/.

[86] Jenna McGregor, "Turning the Tables on a Top-down Military Culture," *Washington Post*, April 16, 2011, https://www.washingtonpost.com/national/on-leadership/2013/04/16/7dbd802a-a6ad-11e2-8302-3c7e0ea97057_story.html.

[87] Ibid.

leadership may be likely to influence improvements in terms of gender within the cyber war arena.

Furthermore, actual demographics show that numbers of personnel in cyber war include relatively high numbers of women as well as racial minorities. [88] This may indicate that cyber war leadership—whether in terms of the general organizational culture that their personalities, demeanor, communication, et cetera foster, or as a result of specific directives or initiatives in an effort to do so, or both—has to some degree successfully shaped an organizational culture conducive to inclusivity in terms of gender, as well as broader diversity. Though toeing the line to ensure that security measures reasonably allow continuing the free flow of idea exchange in cyber space may be challenging, U.S. cyber war leadership appears to be doing so at least somewhat successfully based on these indications.

The Cyber War Workforce in the U.S. Government

The second type of government official entity of cyber warriors consists of cyber security work force personnel who conduct the leg work in order to play out the high level cyber warfare decisions that the leaders make. Within the U.S. government, this mainly includes personnel from the National Security Administration (NSA), Department of Homeland Security (DHS), and Department of Defense (DOD). Within the Department of Defense, the most relevant entities are the U.S. Cyber Command including its reporting entities of U.S. Fleet Cyber Command in the Navy,[89] Army Cyber Command, Air Force Cyber Command, and Marine Forces Cyber

---

[88] "Employment - September 2015 - IBM Cognos PowerPlay Studio," accessed January 24, 2016, http://www.fedscope.opm.gov/ibmcognos/cgi-bin/cognosisapi.dll.

[89] "Thesis on Cyber War - Seeking Advice on Resources."

Command.[90] Another newly established and important group is the Cyber Threat Intelligence Integration Center (CTIIC), under the Director of National Intelligence.[91] [92]

National Security Agency (NSA). While the United States National Security Agency (NSA) is an integral component of the pool of cyber warriors within the U.S. government, obtaining information about cyber warriors within NSA is particularly limited, due to security constraints.[93] The NSA "provides products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners,"[94] as well as "[delivering] critical strategic and tactical information to war planners and war fighters."[95] Its two key missions are Information Assurance, which is essentially defensive; and Signals Intelligence which includes intelligence and supporting military operations,[96] which could include activities considered offensive, or supporting offensive activities. Limited information is publicly available about employees the NSA, let alone specifically about employees of its Signals Intelligence unit.

However, some general observations do shed some light about this group of cyber warriors. Former NSA Deputy Director John Chris Inglis described employees of the agency as

---

[90] "U.S. Cyber Command - U.S. Strategic Command."

[91] "Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center."

[92] "FACT SHEET: Cyber Threat Intelligence Integration Center," *Whitehouse.gov*, February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

[93] Mark Ambinder, "What the NSA's Massive Org Chart (Probably) Looks Like," Defense One, August 14, 2013, http://www.defenseone.com/ideas/2013/08/what-nsas-massive-org-chart-probably-looks/68642/.

[94] "About NSA - National Security Agency/Central Security Service," National Security Agency Central Security Service, accessed February 19, 2016, https://www.nsa.gov/about/index.shtml.

[95] Ibid.

[96] Ibid.

largely introverted.[97] A formerly top secret document outlining NSA culture describes its workforce as historically tending to focus intently on one specific subject area for long swaths of one's career, and relatedly a tendency for resisting change,[98] and "not rocking the boat."[99] This inclination could risk limited organizational openness to gender sensitivity and consideration of historically underrepresented groups within the workforce.

Budget constraints, as well as competition with the private sector in recruiting technologically-savvy personnel have also been characteristic of NSA culture,[100] as well as ambiguity about identifying top expertise in new technologies and technological techniques. Since the 1990s, "people stopped automatically turning to the highly experienced expert, since too often there wasn't one yet."[101] As fear and self-preservation can lead to stereotyping others,[102] ambiguity and competition in the context of NSA culture may lead personnel to quickly judge or dismiss groups who identify differently than they do in terms of gender or other characteristics. Furthermore, NSA culture is observed to be characteristic of quick decision-making, as "Real-time intelligence on life-threatening situations required an emphasis on speed rather than (not opposed to) accuracy."[103] Having to make decisions in a fast-paced environment

---

[97] Camille Tuutti, "National Security Agency Celebrates Diversity, Introverts -- FCW," FCW: The Business of Federal Technology - Circuit, April 16, 2012, https://fcw.com/blogs/circuit/2012/04/fedsmc-chris-inglis-federal-workforce.aspx.

[98] "(U) NSA Culture, 1980s to the 21st Century--a SID Perspective," 79, accessed February 19, 2016, https://www.nsa.gov/public_info/_files/cryptologic_quarterly/NSA_Culture.pdf.

[99] Ibid., 81.

[100] Ibid.

[101] Ibid., 82.

[102] Charles Ramirez-Berg, "Categorizing the Other: Stereotypes and Stereotyping," in *Latino Images in Film: Stereotypes, Subversion, Resistance* (Austin: University of Texas Press, 2002), 13–37, http://www.asu.edu/courses/lia294a/total-readings/RamirezBerg--Categorizing.htm.

[103] "(U) NSA Culture, 1980s to the 21st Century--a SID Perspective," 83.

with many unknowns as well as competition may be likely to influence personnel to fall back on stereotypical thinking, rather than inclusivity and openness, creating a challenging environment in terms of gender equality. However, as the commander of both NSA and U.S. Cyber Command stated as of early 2016, significant structural reorganization of NSA will be soon emerging,[104] indicating that organizational cultural change may likely be on the horizon along with it.

Department of Homeland Security. The Department of Homeland Security's role in cyber security is to lead protecting the United States,[105] which essentially infers a defensive role in cyber war. In the event of a cyber war attack on the U.S., DHS would likely be the key coordinator of expertise entities within the federal government. Unlike NSA's orientation as an intelligence entity, and DoD's as a military entity, DHS is positioned as a civilian entity. In DHS lie several cyber security-related entities within one another, largely under the Office of Cybersecurity and Communications, which houses the National Cybersecurity and Communications Integration Center,[106] and within it the United States Computer Emergency Readiness Team (US-CERT);[107] as well as the research-focused Cyber Security Division.[108]

In terms of a gender perspective, DHS's status as a civilian entity would likely subject it at least somewhat more than DoD, for example, to nonmilitary-related gendered characteristics. DHS may have more flexibility in how it describes itself and its workforce, and how it shapes its

---

[104] Sean Lyngaas, "NSA's Information Assurance Directorate at a Crossroads," *FCW: The Business of Federal Technology*, January 26, 2016, https://fcw.com/articles/2016/01/26/nsa-iad-lyngaas.aspx.

[105] "U.S. Federal Cybersecurity Operations Team: National Roles and Responsibilities."

[106] "National Cybersecurity and Communications Integration Center | US-CERT," *Official Website of the Department of Homeland Security, United States Computer Emergency Readiness Team*, accessed February 20, 2016, https://www.us-cert.gov/nccic.

[107] "About Us | US-CERT," *Official Website of the Department of Homeland Security*, accessed February 20, 2016, https://www.us-cert.gov/about-us.

[108] "Cyber Security Division | Homeland Security," *U.S. Department of Homeland Security*, accessed February 20, 2016, https://www.dhs.gov/science-and-technology/cyber-security-division.

own organizational culture, in ways that may impact gendered aspects. For instance, a report by the Homeland Security Culture Task Force recommended that DHS change its language replacing 'Human Capital' with 'employees' or 'members,' in efforts to more effectively empower its staff.[109] This language has potential to better foster an inclusive environment to contributors of all genders. Furthermore, the culture task force recommended fostering a mindset "driven to challenge 'conventional thinking' and with a 'license' from the Secretary to champion imaginative/innovative processes and ideas,"[110] as well as encouraging a multifaceted organizational culture,[111] and institutionalizing opportunities to be innovative.[112] If adopted, these organizational characteristics would also promote an inclusive, gender-sensitive environment. However, whether and to what degree such recommendations are actually implemented in practice remains ambiguous, and depends on many aspects of the organization such as social interactions between mentors and mentees that ultimately shape culture.[113]

DHS has several aspects to its cyber security workforce recruitment and education efforts.[114] A recruitment video for cybersecurity jobs emphasizes nationalistic integrity, and depicts the technological work as critical to national security. The video is shot with blue colored

---

[109] "Report of the Homeland Security Culture Task Force" (Homeland Security Advisory Council, Homeland Security Culture Task Force, January 2007), 2–3, https://www.dhs.gov/xlibrary/assets/hsac_ctfreport_200701.pdf.

[110] Ibid., 5.

[111] Ibid., 6.

[112] Ibid., 8.

[113] MikeNCM, "In Homeland Security, Mentoring Diffuses Organizational Culture," *Medium*, October 18, 2015, https://medium.com/homeland-security/in-homeland-security-mentoring-diffuses-organizational-culture-60bd83737b2b#.3c8ls270k.

[114] "DHS Cybersecurity Careers | Homeland Security," *Official Website of the Department of Homeland Security*, accessed February 20, 2016, https://www.dhs.gov/homeland-security-careers/dhs-cybersecurity.

filtering,[115] which is used in cinematography to depict a mood of coldness, uncertainty, and also safety, and often of military environments.[116] Although DHS is technically civilian in orientation, it could be seen as depicting itself, and even promoting itself, as having similar qualities as military entities. If it were to adopt a traditional military culture oriented toward an overarchingly masculine kinetic war framework, this may make it difficult to adopt the inclusive environment that the culture task force recommended it strive to adopt. However, given recent indications that the U.S. military and particularly cyber entities within it have been evolving toward a more inclusive culture that would lend itself positively in terms of gender, as discussed in other sections of this analysis, DHS mirroring those aspects of military culture may positively promote increased gender equality.

Department of Defense – United States Cyber Command. The U.S. Department of Defense, and specifically U.S. Cyber Command (USCYBERCOM) within DoD, is considered by many as the main lead in American cyber war activity.[117] U.S. Cyber Command is situated under U.S. Strategic Command, and entails service elements of Army Cyber Command, Fleet Cyber Command in the Navy, Air Force Cyber Command, and Marine Forces Cyber Command.[118] USCYBERCOM also has a reporting relationship with the Coast Guard Cyber Command, though the Coast Guard officially is subordinate to DHS.[119]

However, despite clear-cut organizational charts and other specified descriptions, how U.S. Cyber Command fits into the larger organizational construct of the U.S. military is unclear

[115] *Careers in Cybersecurity | Homeland Security*, 2012, https://www.dhs.gov/video/careers-cybersecurity.

[116] Isaac Botkin, "Color Theory for Cinematographers," *IsaacBotkin.com*, March 6, 2009, http://isaacbotkin.com/2009/03/color-theory-for-cinematographers/.

[117] Reveron, "Cyberspace and International Security Class - Government E-1743."

[118] "U.S. Cyber Command - U.S. Strategic Command."

[119] Ibid.

even to those who are directly involved in and part of it. For example, a Freedom of Information Act inquiry requesting personnel demographics of those employed with U.S. Cyber Command resulted in a staff member specifically mentioning surprise that the Air Force District of Washington Civilian Personnel Office holds the information, rather than USCYBERCOM itself.[120] In the real world, and especially in a still newly established arena such as cyber war, the ways in which people orient themselves and institutions do not always perfectly reflect how they are described on paper.

As of late 2012, USCYBERCOM was cited to have had 27,000 staff.[121] Employment trends of the U.S. Army Cyber Command show an incrementally increasing number of staff from 2014 through 2015.[122] The ages of Army Cyber Command personnel has weighed more heavily toward those ages 45-49, of which there were four times as many staff than those between ages 25-29, and a middle amount in ages 30-44,[123] despite oft-cited stereotypes of cyber warriors and hackers being very young.

About one third, or 32.6% of USCYBERCOM employees were female.[124] Although a one-third proportion is fewer females than would represent the ratio of the general population being about half women, this proportion of female cyber warriors still defies often discussed stereotypes of cyber experts being overwhelmingly male. Furthermore, 26% of professional

---

[120] Kendall Cooper, "Request of USCYBERCOM Personnel Demographics," accessed February 14, 2016, https://mail.google.com/mail/u/0/#inbox/1524f7acb4429a3c.

[121] The Economist, *Richard A. Clarke*.

[122] "Employment - September 2015 - IBM Cognos PowerPlay Studio."

[123] Ibid.

[124] Ibid.

computing occupations in the U.S. have been held by women as recently as 2013,[125] meaning that the proportion of female cyber warriors is higher than the percentage of women overall working in information technology roles. This could be due to robust diversity recruitment efforts by the U.S. cyber military entities, in comparison to private and other sectors of recruitment of women to IT positions. In terms of a gender analysis, although the proportion of cyber warrior positions is not equivalent to the proportion of women and men in the general population, the ratio of women cyber warriors in US Army Cyber Command is notably closer to it than that of women in IT positions overall in the U.S.

Regarding diversity, 36.8% of personnel in US Army Cyber command were minorities as of September 2015.[126] Racial minorities accounted for 22.5% of the U.S. population as of 2014,[127] meaning that US Army Cyber Command personnel is more racially diverse than the overall population. This also is contrary to stereotypes often mentioned in cyber war literature, that cyber war hackers tend to be white. In terms of a gender analysis, based on demographic information available, the actual population of cyber warriors appears to be not only more equal in terms of gender than the overall technology workforce sector, but also more diverse racially. In other words, way the existing cyber war literature describes cyber war does not reflect what the more diverse demographics about *actual* cyber warriors seems to show.

How an organization describes itself is at least as significant as demographic statistics about who it actually consists of. The Navy's strategy and operationalization of cyber warfare

---

[125] "Women and Information Technology By the Numbers," *National Center for Women & Information Technology*, February 28, 2014, http://www.ncwit.org/sites/default/files/resources/btn_02282014web.pdf.

[126] "Employment - September 2015 - IBM Cognos PowerPlay Studio."

[127] "USA QuickFacts from the US Census Bureau," *United States Census Bureau*, accessed February 21, 2016, http://quickfacts.census.gov/qfd/states/00000.html.

are outlined by the Information Dominance Corps.[128] Cyber war is described in essentially the same or equivalent terminology as traditional war, regarding how descriptions and wording are oriented in militarized ways. Concerning a gendered perspective, even cyber war strategy and operationalization being positioned under the umbrella of 'Information Dominance Corps' could be considered gendered. For example, Richard Clarke refers to the word 'dominance' being used by the military as not only arrogant, but also sexual in nature, in a way that does not seem to make sense in the context.[129] Usage of this verbiage may shape an environment that is perceived as unwelcoming to women, given that sexualized vocabulary, even if only subliminally so, may promote male dominance.[130]

However, at the time of writing, U.S. Cyber Fleet Commander Vice Admiral Jan Tighe is currently surveying what the Navy calls 'information warriors' about how best to rename the Information Dominance Corps, suggesting that the term 'Cryptologic Warfare' may be more fitting. [131] Significant for a gender analysis viewpoint, terms that do not reflect women's experiences and worldviews can contribute to social male hegemony and patriarchy, and thus undermine gender equality.[132] [133] However, creating new terminology can make a considerable

---

[128] United States Navy, "Information Dominance Corps," *United States Naval Academy Center for Cyber Security Studies*, accessed February 15, 2016, http://www.usna.edu/CyberCenter//_files/documents/idc/IDC_Overview.pdf.

[129] The Economist, *Richard A. Clarke*.

[130] Jennifer Saul, "Feminist Philosophy of Language," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Winter 2012, 2012, http://plato.stanford.edu/archives/win2012/entries/feminism-language/.

[131] Tighe, "Vice Admiral Tighe's Letter to the Information Warrior Community.pdf."

[132] Miranda Fricker, *Epistemic Injustice* (Oxford University Press, 2007), 155, http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780198237907.001.0001/acprof-9780198237907.

[133] Saul, "Feminist Philosophy of Language."

difference in bringing to light women's experiences and signifying to the hegemonic group aspects that are significant to women but may not be visible to other groups.[134] [135]

Consequently, there are direct efforts, not only supported but lead by U.S. cyber warfare leadership, to more accurately and inclusively brand itself, which is likely to impact the overarching culture of cyber warriors in turn. Furthermore, this initiative indicates how cyber warriors and cyber warfare are currently perceived among the military cyber warfare community itself, as well as their perceptions about the path in which cyber warfare is moving forward. The U.S. Navy branch of cyber warfare appears to be not only overtly recognizing that the current terminology is insufficient and unsuitable in describing itself, but it is actively working toward improving its self-descriptive language to be not only more inclusive, but also what it deems as more accurate in order to reflect its work and workforce. Moreover, the process through which it is going about determining what specific terminology it will use moving forward appears to be an overall open process, endeavoring to include relevant individuals and groups that are directly involved in the work in question, and doing so in ways that are as accessible as possible to them.

For example, the letter from Vice Admiral Tighe specifically mentions multiple avenues through which personnel can access the survey to voice their opinions on new terminology and explain reasoning behind it, and provides multiple URL addresses for various webpages through which they can do so.[136] This includes URLs to social media pages, specifically on Twitter and Facebook,[137] signifying an effort that Navy cyber leadership is reaching out through avenues that those being surveyed can easily access, are comfortable using, and likely often use personally.

---

[134] Ibid.

[135] Fricker, *Epistemic Injustice*, 155.

[136] Tighe, "Vice Admiral Tighe's Letter to the Information Warrior Community.pdf."

[137] Ibid.

The meaning behind offering access to the survey through these multiple channels suggests a concerted effort to gather honest feedback, and efforts to obtain it through communication channels with which the surveyed population is most comfortable and can easily access.

Options on the survey for the most important factors for renaming it include aligning with enlisted workforce, embracing the Navy's cryptological heritage, encompassing all core mission areas, and reflecting its 'evolution from a passive role to a fires and effects role in a warfare domain'.[138] Interestingly, this suggests that the current terminology is perceived to potentially *not* encompass all the related core mission areas, nor align with enlisted workforce positions. Moreover, it reveals a perception of information warfare as having developed further into being active rather than passive in terms of warfare, or in other words, further toward an offensive rather than limited to being largely a defensive warfare domain.

Within the military, educational entities focusing on training personnel toward proficiency in cyber war skills and tactics are an important aspect of the larger base of cyber warriors. The U.S. Naval Academy holds a Center for Cyber Security Studies,[139] and the Air Force Information Operations School also has a focus on training cyber warriors.[140] Videos that appear to be created largely for recruitment purposes shed some light on how such military education entities view, describe, and depict themselves.

In a similar fashion to the DHS video recruiting cyber savvy personnel mentioned earlier, a video about the Air Force Information Operations School emphasizes the importance and significance of cyber warfare and the corresponding need for growth in the cyber war workforce,

---

[138] "Information Warfare Designator Name Change Survey," accessed February 21, 2016, https://www.surveymonkey.com/r/F35YRJ9.

[139] "Center for Cyber Security Studies: USNA," *United States Naval Academy*, accessed February 19, 2016, http://www.usna.edu/CyberCenter/.

[140] United States Department of Defense, *The Making of a Cyber Warrior - DoD News*.

as well as overarching nationalistic pride.[141] Several students of the institution are interviewed throughout the video, whose appearances seem to roughly reflect the actual, fairly diverse, demographics of the cyber security workforce within USCYBERCOM. Instructors and officers describe cyber war [142] in a way that seems to intend to validate it as an exciting and important type of warfare, implying that people may not assume it to be exciting and important to begin with. Similar to other general military recruitment media in the 1990s and 2000s, cyber warrior recruitment media emphasizes how critical the positions are to defend America, evoking nationalist and perhaps even paternalistic sentiment. In what could be an attempt to counter balance perceived notions about computer work being mundane and undervalued,[143] [144] it also depicts a sense of adventure and excitement. Interestingly, this effort to emphasize cyber warriors as outward-oriented contrasts, perhaps purposefully, with previously mentioned observations about the workforce of NSA being largely introverted.

One officer emphasizes cyber security work being "not just another support mission," but rather more highly valued, viewing it as, "Ops…another tool…to utilize in defending freedom and keeping America safe."[145] If support work is considered feminine, by means of office secretarial work having been traditionally done by women since the early to mid-twentieth

---

[141] Ibid.

[142] Ibid.

[143] Hadi Hadi Partovi, "Why Is Computer Science Generally Viewed As 'Uncool' By Teenagers?," April 15, 2014, http://www.forbes.com/sites/quora/2014/04/15/why-is-computer-science-generally-viewed-as-uncool-by-teenagers/#43b6080ac984.

[144] Sapna Cheryan, "Debunking Stereotypes: Ways to Change the Image of Computer Science" (University of Washington Department of Psychology: Stereotypes, Identity and Belonging Lab), accessed February 28, 2016, http://depts.washington.edu/sibl/Publications/Debunking%20Stereotypes%20Brochure%20(teacher).pdf.

[145] United States Department of Defense, *The Making of a Cyber Warrior - DoD News*.

century,[146] [147] this emphasis of cyber security work being more important than that, could be viewed as attempting to make it seem more masculine. However, at the same time, the video clearly attempts to show diversity in gender as well as race of instructors, officers, and students, seeming to signify an intent to be inclusive beyond the specific demographic groups that stereotypes may assume to be most involved in cyber work.

Another important aspect of the cyber security workforce within the military is that higher numbers of cyber warriors may oscillate during their careers between working for the government and the private sector. The Department of Defense cites that personnel in cyber security positions are moving more frequently across private sector information technology companies and government positions.[148] Although the workforce of U.S. Army Cyber Command shows more promisingly diverse demographics than the overall U.S. technology sector workforce, increased sharing between the two may mix those trends.

Cyber Threat Intelligence Integration Center. The Cyber Threat Intelligence Integration Center (CTIIC) is a most recent addition to the assortment of U.S. government entities specifically relating to cyber war. However, little information is available about it at the time of writing, as its development is still in the works. Once the CTIIC is established, its directive intends it to play

---

[146] Eric Jaffe, "The New Subtle Sexism Toward Women in the Workplace," *Fast Company*, June 2, 2014, http://www.fastcompany.com/3031101/the-future-of-work/the-new-subtle-sexism-toward-women-in-the-workplace.

[147] Sylvia Cutler, "Sexist Job Titles and the Influence of Language on Gender Stereotypes," *Brigham Young University Humanities*, January 16, 2015, http://humanities.byu.edu/sexist-job-titles-and-the-influence-of-language-on-gender-stereotypes/.

[148] "DoD Needs to Improve Cyber Culture, CIO Says > U.S. DEPARTMENT OF DEFENSE > Article View," accessed January 17, 2016, http://www.defense.gov/News-Article-View/Article/626607/dod-needs-to-improve-cyber-culture-cio-says.

a central role in "connecting the dots" for cyber security threats.[149] Although its overall initiative and function are outlined, what specifically the CTIIC will look like remains to be seen.

Gender Analysis of Cyber Warriors within Official U.S. Government Entities. While the cyber warrior community within the U.S. government remains largely militarized in nature, efforts are in the works to establish an environment more inclusive to a wider range of demographics of personnel, which has to a certain degree appeared to be successful. This affects how the workforce of cyber warriors is shaped, how it views itself, and also how private citizens may view cyber war and cyber warriors. Overall principles and characteristics of cyber war that are emphasized are that it is fast-paced; an important aspect of warfare overall and that it will become even more so in the years to come; and varying mentions of innovation, ranging from observations of historically short-sightedness and closed-mindedness about new ways of thinking on one hand, to strong emphasis of the need for innovative mindsets in the cyber warrior workforce on the other. Strategies for the future appear to emphasize the latter, which is encouraging in terms of efforts to increase gender equality and an overall more inclusive assembly of cyber warriors moving forward.

A gender analysis concludes that self-depictions and implications about the culture of cyber warriors remain largely masculine in nature. This is evident from comparing the mood and protective—even paternalistic—quality of military cyber warrior recruitment videos, with traditional conceptions of what is considered 'feminine.' From the lens of long-standing military culture and its orientation around kinetic war, which has overarchingly emphasized concepts of masculinity, shaping cyber warfare to be comparatively more equal in terms of a gender perspective may prove a difficult endeavor.

---

[149] "FACT SHEET."

However, there are efforts within the U.S. government and particularly military cyber war arena to level the playing field from a gendered perspective. These include employing higher numbers of women in cyber warfare jobs, as well as progressive efforts to initiate cultural shifts by changing specific terminology to be more inclusive. These such recent organizational strategies signal tangible intentions for improving conditions in terms of gender equality as well as diversity in the cyber war landscape, despite that doing so is likely to be challenging.

Women may be discouraged from pursuing a career path as a cyber warrior if they view even subliminal, if not overt, characterization of cyber warrior roles as being masculine. Gender indefinitely plays a role in the way technology is used and viewed, as particularly feminist literature examining Western culture has widely discussed. As Pechtelidis, Kosma and Chronaki write, "Technology and the handling of machines have been historically constituted as masculine competencies in patriarchal culture."[150] As a key component of cyber war, a continuingly gendered perception of technology will likely impact not only *whether* women decide to pursue careers as cyber warriors, but if so, *how* they go about pursuing it. Through the latter process, they may potentially even alter how they characterize themselves in order to both fit into cyber war culture while simultaneously maintaining cohesion with how they are viewed in terms of femininity.[151] As one study of female students of information technology in arenas other than cyber culture has found, women who pursue software engineering were more likely to opt for career paths more closely aligned with traditionally female roles, "because they choose to strategically adapt to given gender norms; being fully aware of their subordinated position in a

[150] Yannis Pechtelidis, Yvonne Kosma, and Anna Chronaki, "Between a Rock and a Hard Place: Women and Computer Technology," *Gender and Education* 27, no. 2 (February 10, 2015): 165, doi:10.1080/09540253.2015.1008421.

[151] Ibid.

male-dominated field, they find that this way it is easier to meet social expectations."[152] This may similarly be the case with women pursuing professional roles in cyber war.

As leadership within DoD has pointed out, a significant culture change is needed within the cyber war arena.[153] [154] The environment of cyber warriors is a challenging one to shape. Even as fast-paced as it is, a significant cultural shift will take time, but current efforts appear to indicate movement in a positive direction.

Cyber Warriors of Other States

The United States is far from the only country to have entities capable of conducting cyber warfare. Over 120 states have worked on developing cyber warfare military doctrines.[155] According to cyberwar expert Richard A. Clarke, "The CIA says there are between 20 and 30 countries that have cyber warfare units with significant offensive capability," including China, Russia, Israel, the United Kingdom, Germany, North Korea, and Brazil.[156]

China and Russia are considered the two key states most involved in cyber war other than the U.S.[157] [158] [159] Although information is available about China's and Russia's cyber *strategies*,

---

[152] Ibid.

[153] Lisa Ferdinando, "Cybersecurity Demands Culture Change, DoD Official Says," *U.S. DEPARTMENT OF DEFENSE*, accessed February 21, 2016, http://www.defense.gov/News-Article-View/Article/617767/cybersecurity-demands-culture-change-dod-official-says.

[154] Lisa Ferdinando, "DoD Needs to Improve Cyber Culture, CIO Says," *U.S. Department of Defense*, October 29, 2015, http://www.defense.gov/News-Article-View/Article/626607/dod-needs-to-improve-cyber-culture-cio-says.

[155] Jeffrey Carr, "The Role of Cyber in Military Doctrine," in *Inside Cyber Warfare* (O'Reilly Media, 2009), http://proquest.safaribooksonline.com.ezp-prod1.hul.harvard.edu/book/networking/security/9781449377229/firstchapter#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODE0NDkzNzcyMjklMkZjaGluYV9taWxpdGFyeV9kb2N0cmluZSZxdWVyeT13b21lbg==.

[156] The Economist, *Richard A. Clarke*.

[157] Carr, "The Role of Cyber in Military Doctrine."

including cyber attacks that have been attributed to each of them,[160] [161] [162] there is little information available about Chinese and Russian cyber *warriors*. Without public information from the government or military describing specific cyber initiatives in a way even roughly equivalent to the U.S.'s information about its various cyber war entities, it is difficult to determine much about who these pools of cyber warriors are, what their motivations may be, and so forth, in terms of a gender analysis.

One advantage of a state engaging in cyber attacks and cyber war is plausible deniability,[163] meaning that a state can simply deny that it is responsible for an attack, and it is unclear or even impossible to determine where responsibility for the attack actually lies. Furthermore, it can even in a sense technically be true that a state is not directly responsible for conducting an attack, if for example the attack itself is conducted by individuals or groups unofficially affiliated with the state, rather than actual state entities conducting the attack directly.[164] For example, even if Russia did not actually admit to being responsible for cyber action against Georgia, the effects of a major cyber attack against Georgia during a conflict between the two countries in 2008 clearly benefitted Russian interests.[165] [166] Ultimately, this

---

[158] Clarke and Knake, *Cyber War*, Location 49.

[159] Reveron, *Cyberspace and National Security*.

[160] Ibid.

[161] Clarke and Knake, *Cyber War*.

[162] Carr, "The Role of Cyber in Military Doctrine."

[163] Reveron, "Cyberspace and International Security Class - Government E-1743."

[164] Ibid.

[165] Carr, "The Role of Cyber in Military Doctrine."

aspect of cyber war makes it more difficult to determine who cyber warriors are than it would be to determine who consists of traditional warriors in kinetic war, both in relation to specific attacks, and more broadly in cyber war.

Interestingly, this obscurity about identity may create a sense of freedom for nontraditional demographic groups to engage as cyber warriors in ways that they may not be comfortable doing so in more visible roles as traditional combatants. For example, if a woman is uncomfortable with the idea of engaging in war and becoming a soldier in the traditional sense, such as joining an infantry unit, because of how that role conflicts with traditional female roles and gender norms, she may be more comfortable in a warrior role in cyberspace, where her identity as a woman may not be evident, such as to her adversaries. In terms of a gender analysis, cyberspace provides a unique atmosphere for demographic groups who may have been less visible, either by choice or as a result of being undermined, in the traditional warfare landscape, to play more prominent roles. Whereas in traditional warfare, males typically held positions of power and were considered the key players,[167] cyberspace may alter wartime power dynamics in new directions that more easily lend themselves toward nontraditional groups to hold more powerful roles.

In the larger scope, such shifting power dynamics among the individual players in warfare could in turn transform wartime strategic thinking. Even the vocabulary used in informal conversations about wartime policy are often gendered in ways that designate power relationships between players, and can also be used as an intimidation tactic.[168] Where war

---

[166] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Corporation, 2009), 2, https://books-google-com.ezp-prod1.hul.harvard.edu/books/about/Cyberdeterrence_and_Cyberwar.html?id=MJX6jL6IeF0C.

[167] Braudy, *From Chivalry to Terrorism*.

presents a uniquely dynamic opportunity (ironic though it may sound) for social norms to shift, due for instance to higher numbers of males leaving their communities and along with them opening new role opportunities for more women,[169] [170] cyber war may similarly present new opportunities for women and other groups to take part in new ways than they often have in kinetic war. In other words, cyberwar may be to war, what war is to non-war environments, in terms of enabling social norm shifting. Cyberwar may offer new ways of thinking about war overall, because of the new perspective of nontraditional groups being more involved in war than they have been previously. Although diverse groups can pose their own unique challenges and internal conflicts, they can also enhance creative thinking and problem solving mindsets. [171] This may be the case in cyber war not only if cyber warriors consist of more women than traditional war, but also because cyber warriors are likely to reflect a wider range of types of masculinity, providing further diversity even among masculinities alone.

Russia's Cyber Warriors. The Russian government has been known to hire personnel to conduct activities promoting the government that appear to be done by private citizens on their own personal accord, but are actually paid by the government.[172] For example, on blogs about political issues, in many cases posts can be identified that seem to support the Russian government in a suspiciously positive light, indicating that they are likely not opinions voiced by

---

[168] Cohn, ed. Cooke, and ed. Woollacott, "Wars, Wimps, and Women: Talking Gender and Thinking War.pdf."

[169] Penny Summerfield, "Gender and War in the Twentieth Century," *The International History Review* 19, no. 1 (March 1997): 3–15, doi:10.1080/07075332.1997.9640771.

[170] Goldstein, "War and Gender."

[171] Frances J. Milliken, Caroline A. Bartel, and Terri R. Kurtzberg, "Diversity and Creativity in Work Groups: A Dynamic Perspective on the Affective and Cognitive Processes That Link Diversity and Performance," in *Group Creativity : Innovation through Collaboration*, ed. Paul B. Paulus and Bernard A. Nijstad, accessed February 26, 2016, https://books-google-com.ezp-prod1.hul.harvard.edu/books/about/Group_Creativity_Innovation_through_Coll.html?id=9QE2fXW_ce0C.

[172] Reveron, "Cyberspace and International Security Class - Government E-1743."

choice, but rather posts that individuals are paid to write and publish. [173] Although it differs from the type of cyber war that is often discussed, a government covertly infiltrating arenas intended to house open discourse among citizens, for the purpose of socially influencing government support, could be considered a type of social cyber war strategy. This falls under what is deemed 'information-psychology,'[174] which is an information technology perspective on the long-used warfare tactic of psychology operations, or Psyops.[175] In terms of Russian military strategy use of information-psychology, Timothy Thomas has found that:

> A significant shift in the importance of information and social media has resulted in a slight shift in the pillars of information warfare for some Russian specialists. Instead of information-technical and information-psychological affairs, for example, the focus for some is now on scientific-technical and political-psychological issues.[176]

A specific use of Russia's information psychology in cyber war is evident from the pro-Russian unrest in Ukraine in 2014, during which Russia used strategic communication strategies to undermine support for the Ukrainian backers.[177] Through information psychology tactics, Russian strategists were able to create an impression of a higher level of civilian support for Russian than may actually have existed within Ukraine.[178] Although this approach was used as one part of a larger military strategy, rather than being used as a primary tactic, the psychological

---

[173] Ibid.

[174] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?," *The Journal of Slavic Military Studies* 27, no. 1 (2 January 2014): 101–30, doi:10.1080/13518046.2014.874845.

[175] James Corbett, "Psyops 101: An Introduction to Psychological Operations : The Corbett Report," *The Corbett Report Open Source Intelligence News*, October 23, 2012, https://www.corbettreport.com/psyops-101-an-introduction-to-psychological-operations/.

[176] Thomas, "Russia's Information Warfare Strategy," 102–103.

[177] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," *National Defence Academy of Latvia Center for Security and Strategic Research. Policy Paper*, no. 2 (April 2014): 2002–14.

[178] Ibid.

information aspect impacted public opinion and ultimately is deemed to have affected the eventual outcome of the conflict.[179]

In terms of a gender perspective of cyber war, an emphasis on information psychology may offer an opportunity in the information technology sphere where women may feel more inclined to become involved than in other aspects of cyber war. For example, nearly 72% of psychology doctoral students have been women,[180] which may mean that a psychology perspective on cyber war may likewise appeal to women more strongly than men.[181] In terms of the technology sector in Russia, about 29.7% of those educated in the field of engineering and technology have been women.[182] Perhaps introducing psychology and technology may entice higher numbers of women to enter the technology field.

China's Cyber Warriors. Cyber war literature includes frequent mentions about China's activities in the arena, but little is mentioned or appears to be available about who cyber warriors of China actually are. While specifically who has conducted them has remained unclear, many cyber attacks on the U.S. have originated in China.[183] [184] Although specifics about actual cyber warriors is not readily available, some indications can be gleaned from the pool of potential cyber warriors in China's population. China has a workforce particularly strongly skilled in

---

[179] Ibid.

[180] Amy Cynkar, "The Changing Gender Composition of Psychology," *Http://www.apa.org* 38, no. 6 (June 2007): 46.

[181] As statistics on the rate of women in psychology specifically in Russia could not be found, this figure is based on the United States, in effort to provide a sense of the overall sector of psychology.

[182] Theodore P. Gerber and David R. Schaefer, "Horizontal Stratification of Higher Education in Russia _ Gerber Schaefer.pdf," *Sociology of Education* 77, no. 1 (January 2004): 43.

[183] Reveron, "Cyberspace and International Security Class - Government E-1743."

[184] James Fallows, "Cyber Warriors," *The Atlantic*, March 2010, http://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/.

science, math, and technology, making it a well prepared country for staffing specifically skilled personnel to be cyber warriors.[185]

However, in terms of a gender perspective, China's cyber strategy and employment trends indicate antithetical conclusions around the level of openness to gender sensitivity in this area. Chinese cyber strategy has included rather overtly sexist concepts, such as the 'honey pot' strategy, meaning of using women as sexual objects to distract adversaries.[186] Though this type of gender-biased strategy and terminology undermines women's participation as active participants in cyber war, other indications may hint at movement toward women's increased participation in cyber space. China's technology sector has been dominated by males, but many companies have recently adopted efforts to recruit more women, which has been successful to some degree.[187] That said, it is hard to say whether these trends, largely in the private sector, reflect or may even influence similar efforts in the public sector.

---

[185] Carr, "The Role of Cyber in Military Doctrine."

[186] Carr, *Inside Cyber Warfare*.

[187] Qian Ruisha, "In China's Tech Sector, Women Make Strides amid 'Brogrammer' Culture," *Ecns.cn*, June 16, 2015, http://www.ecns.cn/cns-wire/2015/06-16/169443.shtml.

Chapter III:

Analysis and Conclusions

In terms of final analysis and conclusions drawn from this thesis, firstly existing literature related to cyber war will be discussed. Secondly, a gender analysis of cyber warriors will be discussed, including particular consideration of cyber warriors and military culture, and cyber warriors in countries other than the United States.

Gender Analysis and Conclusions: Existing Literature Related to Cyber War

Existing literature about cyber war discusses a gender perspective extremely minimally, if at all. However, its references to gender do indicate that cyber war scholars have recognized the significance of gender aspects, at least to some degree. Overall, gender analysis is largely absent from discussions about cyber war. Literature on gender and technology indicates that cyber war would be likely to be considered overarchingly—if perhaps subliminally—masculine, given its orientation within the technology sector. Furthermore, literature on gender and war discusses that the field of war and interstate conflict has been largely considered masculine as well, including in how strategizing around war and how specific wartime strategies are discussed and valued. Discussions within the gender and technology, and the gender and war subject areas could lead one to conclude that a gender analysis of cyber warriors would reflect some combination of gendered aspects of traditional soldiers and that of computer experts.

However, several facets of cyber war present a unique new opportunity for further gender equality than both the technology and war sectors separately seem to have shown. Cyber

technology skills may be particularly accessible for women to obtain, which may make work in the cyber war sector easier to pursue than in the technology sector, and in kinetic war roles. Further flexibility in work conditions than traditional combatant roles may also increase women's participation and interest in cyber war, in comparison to their conventionally more minimal participation in kinetic war than men's. Women's increased involvement as cyber warriors in turn could bring further gender equality to the overall war landscape in new ways.

Gender Analysis Conclusions: Cyber Warriors

The landscape of actual cyber warriors within the U.S., as well as how cyber war is characterized by cyber war groups, is more promising in terms of gender equality than literature about gender and technology and gender and war would lead one to expect. U.S. cyber war leaders have initiated some significant actions that are likely to bring improved gender equality and inclusivity to the cyber war landscape, such as initiatives to change currently used terminology. Such direct efforts, not only supported but lead by U.S. cyber warfare leadership, to rebrand itself, is also likely to impact the overarching culture of cyber warriors in turn. Some aspects of organizational culture within U.S. cyber war entities may present challenges, such as a fast-paced environment which may lead personnel to be more likely to fall back on stereotypes. However, several organizational structural changes that are currently in the works may present opportunities for internal cultural shifts that may enhance organizational conditions in terms of gender.

Demographics of actual personnel within U.S. Cyber Command show that cyber warriors within that entity differ from stereotypical views of both personnel within the technology sector,

as well as within the war sector. Staff within U.S. Cyber Command are in older age brackets,[188] have a higher proportion of women than the overall technology sector, [189] [190] and a higher proportion of racial minorities than the U.S. population.[191] [192] These characteristics indicate a more progressive landscape of cyber warriors than literature about cyber war, gender and technology, and gender and war, seem to have projected. In terms of a gender analysis, these demographics show promise for cyber war influencing increased gender equality across not only the cyber war arena, but in ways that may also impact the overall war sector and technology sectors as well, given cyber war's positioning within the intersection of those areas. U.S. Cyber Command being a relatively new entity does present challenges such as confusion in how it is oriented among other longer-existing entities within the U.S. government and military, but it also presents opportunities to shape fairly early on in the development of its culture and ultimately legacy as an organization.

Cyber Warriors and Military Culture

Given cyber warriors' position within state militaries, cyber warriors and military culture are an integral aspect of analyzing cyber warriors from a gender perspective. One aspect that emerges as particularly salient is that military culture and cyber culture differ in some ways, and the intersection of them in cyber war is not always a seamless merge. Even those directly involved in cyber war in the U.S. military, including those in leadership positions, have

---

[188] "Employment - September 2015 - IBM Cognos PowerPlay Studio."

[189] Ibid.

[190] "Women and Information Technology By the Numbers."

[191] "Employment - September 2015 - IBM Cognos PowerPlay Studio."

[192] "USA QuickFacts from the US Census Bureau."

discussed this challenge. As Lieutenant Colonel Gregory Conti, Director of West Point's Cyber Security Research Center, and Lieutenant Colonel Jen Easterly, a member of US Cyber Command Commander's Action Group, have observed,

> …while the Defense Department has endorsed Cyber Command, the kinetic warfighting culture generally has not… However, building the most effective Cyber Command will require fundamentally changing military culture -- specifically how we think about networks and how we manage the talent that we need to leverage these networks for warfighting effects. Uncomfortable, but necessary change will be required…[193]

However, cyber war entities within the U.S. appear to be addressing and attempting to ameliorate these challenges fairly openly.

Cyber Warriors in Countries Other than the United States

Analysis of cyber war and cyber warriors in countries other than the United States that have significant cyber warrior entities presents additional aspects worth discussion. A few aspects salient in Russian cyber warrior culture may make cyber war a particularly enticing environment for women. For example, usage of information psychological tactics in cyber operations may resonate with women, given the considerably high numbers of women in the psychology sector. Although the number of women in the technology sector is much lower, introducing approaches within cyber war strategy such as information psychology may initiate further gender equality in the cyber war sector.

In China, sexist terminology has peppered military strategy, which is likely to create a biased environment and pose difficulty toward gender equality within the cyber war sector by undermining women's roles and in it. The Chinese technology sector has also been largely male.

---

[193] Conti and Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture | Small Wars Journal."

However, technology companies have expressed efforts to recruit higher numbers of women in recent years, the success of which may impact public sector workforce trends to build similar efforts.

The nature of cyber warriors' roles being less visible than traditional soldiers, in a similar way to cyber war overall allowing plausible deniability, presents opportunities for women and other otherwise underrepresented groups to potentially be more comfortable participating in it. By offering easier accessibility for those of demographic groups traditionally less active in warfare and holding fewer powerful roles in warfare, this may lend the cyber war landscape to shift overall wartime gender and power dynamics. Ultimately, demographic shifts in individual players in cyber war could in turn transform strategic wartime thinking. Cyber war may present unique opportunities that could open the possibility for social norms and power dynamics to shift, particularly through increased diversity being a likely instigator that enhances creative thinking and problem solving mindsets.

Conclusions

Overall, this gender analysis concludes that the cyber war landscape holds positive potential for evolving into a fairly gender equal environment. Interestingly, cyber war appears to hold this potential particularly more promisingly than do the kinetic warfare or technology sectors. Previous academic discourse focusing on cyber war, as well as on gender and technology, and gender and war, would lead one to believe that cyber war is considerably biased toward hegemonic masculinity. Evidence demonstrates that cyber war indeed emerges from a background likely to tend in this way.

However, significant initiatives in cyber war leadership, particularly by the U.S. military cyber war community, reveal convincing evidence of efforts to improve inclusion among the cyber warrior workforce that hold promising potential for the future of gender and cyber war. Given that the U.S. military is largely considered to be the world leader in the cyber war arena, its leadership in initiating policies moving gender equality *forward*—rather than enabling it to stay static or even fall backward toward digression, holds potential for impacting cyber war cultural shifts worldwide.

Furthermore, several aspects about working in cyber war may counteract some of the barriers that have deterred women and other minority groups from pursuing roles relating to warfare in other domains, and also in technology. Cyber war may not only lend itself to a more diverse workforce than traditional war and technology have tended to attract, but its resulting more diverse workforce holds potential to bring innovative wartime strategic thinking to the forefront, and also to the technology sector. Cyber war has been identified by many as a new wartime domain requiring new ways of thinking about war and technology. Significantly, cyber war may itself bring a fresh perspective to both the technology sector and wartime mindsets, opening new opportunities for innovation and creative problem solving.

Bibliography

"015 Internet Security Threat Report, Volume 20 - 21347932_GA-Internet-Security-Threat-Report-Volume-20-2015-social_v2.pdf." Accessed January 31, 2016. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

"404 - Error: 404." Accessed January 24, 2016. http://www.dni.gov/index.php/about/organization/ctiic-what-we-do.

"About NSA - National Security Agency/Central Security Service." *National Security Agency Central Security Service*. Accessed February 19, 2016. https://www.nsa.gov/about/index.shtml.

"About Us | US-CERT." *Official Website of the Department of Homeland Security*. Accessed February 20, 2016. https://www.us-cert.gov/about-us.

Ambinder, Mark. "What the NSA's Massive Org Chart (Probably) Looks Like." *Defense One*, August 14, 2013. http://www.defenseone.com/ideas/2013/08/what-nsas-massive-org-chart-probably-looks/68642/.

Andres, Richard A., and Derek S. Reveron ed. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Kindle edition., Location 1936–2321. Georgetown University Press, 2012.

Andres, Richard B. "The Emerging Struccture of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and*

Power in a Virtual World, edited by Derek S. Reveron, Kindle Edition., Location 1936–2321. Washington, DC: Georgetown University Press, 2012.

Bar-Yosef, Rivka Weiss, and Dorit Padan-Eisenstark. "Role System Under Stress: Sex-Roles in War." *Social Problems* 25, no. 2 (December 1, 1977): 135–45. doi:10.2307/800290.

Basow, Susan A. "Student Evaluations of College Professors: When Gender Matters." *Journal of Educational Psychology* 87, no. 4 (1995): 656–65. doi:10.1037/0022-0663.87.4.656.

Bērziņš, Jānis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." *National Defence Academy of Latvia Center for Security and Strategic Research. Policy Paper*, no. 2 (April 2014): 2002–14.

Bird, Chloe E., and Patricia P. Rieker. "Gender Matters: An Integrated Model for Understanding Men's and Women's Health." *Social Science & Medicine* 48, no. 6 (March 1999): 745–55. doi:10.1016/S0277-9536(98)00402-X.

Blank, Laurie R. "International Law and Cyber Threats from Non-State Actors." *International Law Studies, U.S. Naval War College* 89, no. 406 (2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2194180.

Botkin, Isaac. "Color Theory for Cinematographers." *IsaacBotkin.com*, March 6, 2009. http://isaacbotkin.com/2009/03/color-theory-for-cinematographers/.

Braudy, Leo. *From Chivalry to Terrorism: War and the Changing Nature of Masculinity*. Kindle Edition. Vintage, 2010.

Careers in Cybersecurity | Homeland Security, 2012. https://www.dhs.gov/video/careers-cybersecurity.

Carr, Jeffrey. *Inside Cyber Warfare*. 1st ed. Sebastopol, Calif: O'Reilly Media, 2010.

———. “The Role of Cyber in Military Doctrine.” In *Inside Cyber Warfare*. O’Reilly Media, 2009. http://proquest.safaribooksonline.com.ezp-prod1.hul.harvard.edu/book/networking/security/9781449377229/firstchapter#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODE0NDkzNzcyMjklMkZjaGluYV9taWxpdGFyeV9kb2N0cmluZSZxdWVyeT13b21lbg==.

“Center for Cyber Security Studies: USNA.” *United States Naval Academy*. Accessed February 19, 2016. http://www.usna.edu/CyberCenter/.

Cheryan, Sapna. “Debunking Stereotypes: Ways to Change the Image of Computer Science.” University of Washington Department of Psychology: Stereotypes, Identity and Belonging Lab. Accessed February 28, 2016. http://depts.washington.edu/sibl/Publications/Debunking%20Stereotypes%20Brochure%20(teacher).pdf.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. Kindle edition. HarperCollins e-books, 2010.

Cohn, Carol, Miriam ed. Cooke, and Angela ed. Woollacott. “Wars, Wimps, and Women: Talking Gender and Thinking War.pdf.” In *Gendering War Talk*, 227–46. Princeton, New Jersey: Princeton University Press, 1993.

Colarik, Andrew M. *Cyber Terrorism : Political and Economic Implications*. Hershey, PA: Idea Group Pub, 2006.

Consalvo, Mia. “Cyberfeminism.” *Encyclopedia of New Media*. Thousand Oaks, CA: Sage Reference, 2002. http://study.sagepub.com/sites/default/files/Ch17_Cyberfeminism.pdf.

Conti, Gregory, and Jen Easterly. “Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture | Small Wars Journal.” *Small Wars Journal*, July 29,

2010. http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture.

Cooper, Kendall. "Request of USCYBERCOM Personnel Demographics." Accessed February 14, 2016. https://mail.google.com/mail/u/0/#inbox/1524f7acb4429a3c.

Corbett, James. "Psyops 101: An Introduction to Psychological Operations : The Corbett Report." *The Corbett Report Open Source Intelligence News*, October 23, 2012. https://www.corbettreport.com/psyops-101-an-introduction-to-psychological-operations/.

Cutler, Sylvia. "Sexist Job Titles and the Influence of Language on Gender Stereotypes." *Brigham Young University Humanities*, January 16, 2015. http://humanities.byu.edu/sexist-job-titles-and-the-influence-of-language-on-gender-stereotypes/.

"Cyber Security Division | Homeland Security." *U.S. Department of Homeland Security*. Accessed February 20, 2016. https://www.dhs.gov/science-and-technology/cyber-security-division.

"Cyber Warfare Lexicon - A Language to Support the Development, Testing, Planning, and Employment of Cyber Weapons and Other Modern Warfare Capabilities." USSTRATCOM, January 5, 2009.

Cynkar, Amy. "The Changing Gender Composition of Psychology." *Http://www.apa.org* 38, no. 6 (June 2007): 46.

"DHS Cybersecurity Careers | Homeland Security." *Official Website of the Department of Homeland Security*. Accessed February 20, 2016. https://www.dhs.gov/homeland-security-careers/dhs-cybersecurity.

Diamond, Larry. “What Is Democracy?” Hilla University for Humanistic Studies, January 21, 2004. http://web.stanford.edu/~ldiamond/iraq/WhaIsDemocracy012004.htm.

“DoD Needs to Improve Cyber Culture, CIO Says > U.S. DEPARTMENT OF DEFENSE > Article View.” Accessed January 17, 2016. http://www.defense.gov/News-Article-View/Article/626607/dod-needs-to-improve-cyber-culture-cio-says.

“Employment - September 2015 - IBM Cognos PowerPlay Studio.” Accessed January 24, 2016. http://www.fedscope.opm.gov/ibmcognos/cgi-bin/cognosisapi.dll.

“FACT SHEET: Cyber Threat Intelligence Integration Center.” *Whitehouse.gov*, February 25, 2015. https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

Fallows, James. “Cyber Warriors.” *The Atlantic*, March 2010. http://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/.

Ferdinando, Lisa. “Cybersecurity Demands Culture Change, DoD Official Says.” *U.S. DEPARTMENT OF DEFENSE*. Accessed February 21, 2016. http://www.defense.gov/News-Article-View/Article/617767/cybersecurity-demands-culture-change-dod-official-says.

———. “DoD Needs to Improve Cyber Culture, CIO Says.” *U.S. Department of Defense*, October 29, 2015. http://www.defense.gov/News-Article-View/Article/626607/dod-needs-to-improve-cyber-culture-cio-says.

Fernbach, Amanda. “The Fetishization of Masculinity in Science Fiction: The Cyborg and the Console Cowboy.” *Science Fiction Studies* 27, no. 2 (July 2000): 234–55.

Fricker, Miranda. *Epistemic Injustice*. Oxford University Press, 2007. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780198237907.001.0001/acprof-9780198237907.

Garber, Megan. "Saving the Lost Art of Conversation." *The Atlantic*, February 2014. http://www.theatlantic.com/magazine/archive/2014/01/the-eavesdropper/355727/.

Gerber, Theodore P., and David R. Schaefer. "Horizontal Stratification of Higher Education in Russia _ Gerber Schaefer.pdf." *Sociology of Education* 77, no. 1 (January 2004): 32–59.

Gertz, Bill. "Ashton Carter Outlines Acts of Cyber War." *The Washington Times*, February 4, 2015, sec. News - Inside the Ring. http://www.washingtontimes.com/news/2015/feb/4/inside-the-ring-ashton-carter-denies-north-korea-c/.

———. "Carter Defines Acts of Cyber War," February 5, 2015. http://freebeacon.com/national-security/carter-defines-acts-of-cyber-war/.

Goldstein, Joshua S. "War and Gender." In *Encyclopedia of Sex and Gender*, edited by Carol R. Ember and Melvin Ember, 107–16. Springer US, 2003. http://link.springer.com.ezp-prod1.hul.harvard.edu/referenceworkentry/10.1007/0-387-29907-6_11.

Hackett, Robert. "Gasp! China Admits to Having Cyber Warriors." *Fortune*, March 26, 2015. http://fortune.com/2015/03/26/china-admits-cyber-warriors/.

Haraway, Donna. "A Cyborg Manifesto: Science, Technolgy, and Socialist Feminism in the Late Twentieth Century." In *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge, 1991.

"Information Warfare Designator Name Change Survey." Survey, February 12, 2016. https://www.surveymonkey.com/r/F35YRJ9.

"Information Warfare Designator Name Change Survey." Accessed February 21, 2016. https://www.surveymonkey.com/r/F35YRJ9.

"Internal DoD Effort Focuses on Individual Cybersecurity Responsibility > U.S. DEPARTMENT OF DEFENSE > Article View," October 14, 2015. http://www.defense.gov/News-Article-View/Article/622987/internal-dod-effort-focuses-on-individual-cybersecurity-responsibility.

Jaffe, Eric. "The New Subtle Sexism Toward Women in the Workplace." *Fast Company*, June 2, 2014. http://www.fastcompany.com/3031101/the-future-of-work/the-new-subtle-sexism-toward-women-in-the-workplace.

Kirby, Paul, and Marsha Henry. "Rethinking Masculinity and Practices of Violence in Conflict Settings." *International Feminist Journal of Politics* 14, no. 4 (December 2012): 445–49. doi:10.1080/14616742.2012.726091.

Lawrence, Dune. "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016." *BloombergView*, April 15, 2014. http://www.bloomberg.com/bw/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: Rand Corporation, 2009. https://books-google-com.ezp-prod1.hul.harvard.edu/books/about/Cyberdeterrence_and_Cyberwar.html?id=MJX6jL6IeF0C.

Lyngaas, Sean. "NSA's Information Assurance Directorate at a Crossroads." *FCW: The Business of Federal Technology*, January 26, 2016. https://fcw.com/articles/2016/01/26/nsa-iad-lyngaas.aspx.

Mazanec, Brian M. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. U of Nebraska Press, 2015.

McGregor, Jenna. "Turning the Tables on a Top-down Military Culture." *Washington Post*, April 16, 2011. https://www.washingtonpost.com/national/on-leadership/2013/04/16/7dbd802a-a6ad-11e2-8302-3c7e0ea97057_story.html.

MikeNCM. "In Homeland Security, Mentoring Diffuses Organizational Culture." *Medium*, October 18, 2015. https://medium.com/homeland-security/in-homeland-security-mentoring-diffuses-organizational-culture-60bd83737b2b#.3c8ls270k.

Miles, Donna. "Defense.gov News Article: Cyber Command Builds 'Cyber Warrior' Capabilities," September 27, 2011. http://archive.defense.gov/news/newsarticle.aspx?id=65459.

Milliken, Frances J., Caroline A. Bartel, and Terri R. Kurtzberg. "Diversity and Creativity in Work Groups: A Dynamic Perspective on the Affective and Cognitive Processes That Link Diversity and Performance." In *Group Creativity : Innovation through Collaboration*, edited by Paul B. Paulus and Bernard A. Nijstad. Accessed February 26, 2016. https://books-google-com.ezp-prod1.hul.harvard.edu/books/about/Group_Creativity_Innovation_through_Coll.html?id=9QE2fXW_ce0C.

Moran, Mary H. "Gender, Militarism, and Peace-Building: Projects of the Postconflict Moment." *Annual Review of Anthropology* 39, no. 1 (October 21, 2010): 261–74. doi:10.1146/annurev-anthro-091908-164406.

"National Cybersecurity and Communications Integration Center | US-CERT." *Official Website of the Department of Homeland Security, United States Computer Emergency Readiness Team*. Accessed February 20, 2016. https://www.us-cert.gov/nccic.

Oakley, Ann. "Women and Children First and Last: Parallels and Differences between Children's and Women's Studies." In *Children's Childhoods: Observed And Experienced*, edited by Berry Mayall, 13–32. Routledge, 2002.

Partovi, Hadi. "Why Is Computer Science Generally Viewed As 'Uncool' By Teenagers?," April 15, 2014. http://www.forbes.com/sites/quora/2014/04/15/why-is-computer-science-generally-viewed-as-uncool-by-teenagers/#43b6080ac984.

Pechtelidis, Yannis, Yvonne Kosma, and Anna Chronaki. "Between a Rock and a Hard Place: Women and Computer Technology." *Gender and Education* 27, no. 2 (February 10, 2015): 164–82. doi:10.1080/09540253.2015.1008421.

"Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center." *Whitehouse.gov*, February 25, 2015. https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

Radziwill, Yaroslav [author. *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden ; Boston: Brill Nijhoff, 2015, 2015.

Ramirez-Berg, Charles. "Categorizing the Other: Stereotypes and Stereotyping." In *Latino Images in Film: Stereotypes, Subversion, Resistance*, 13–37. Austin: University of Texas Press, 2002. http://www.asu.edu/courses/lia294a/total-readings/RamirezBerg--Categorizing.htm.

"Report of the Homeland Security Culture Task Force." Homeland Security Advisory Council, Homeland Security Culture Task Force, January 2007. https://www.dhs.gov/xlibrary/assets/hsac_ctfreport_200701.pdf.

Reveron, Derek. "Cyberspace and International Security Class - Government E-1743." Harvard University Extension School, February 14, 2015.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Edited by Derek Reveron. Kindle edition. Georgetown University Press, 2012.

Roter, Debra L., and Judith A. Hall. "Why Physician Gender Matters in Shaping the Physician-Patient Relationship." *Journal of Women's Health* 7, no. 9 (November 1, 1998): 1093–97. doi:10.1089/jwh.1998.7.1093.

Ruisha, Qian. "In China's Tech Sector, Women Make Strides amid 'Brogrammer' Culture." *Ecns.cn*, June 16, 2015. http://www.ecns.cn/cns-wire/2015/06-16/169443.shtml.

Saul, Jennifer. "Feminist Philosophy of Language." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Winter 2012., 2012. http://plato.stanford.edu/archives/win2012/entries/feminism-language/.

Sax, Leonard. *Why Gender Matters: What Parents and Teachers Need to Know about the Emerging Science of Sex Differences*. Potter/TenSpeed/Harmony, 2007.

Scott, Joan W. "Gender: A Useful Category of Historical Analysis." *The American Historical Review* 91, no. 5 (December 1986): 1053–75.

Serabian Jr., John A. "Cyber Threats and the US Economy." Central Intellligence Agency, February 23, 2000. News & Information, Speeches & Testimony Archive 2000.

https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

Shantz, Jeff [author. *Cyber Disobedience : Re://presenting Online Anarchy*. Winchester, UK ; Washington, USA: Zero Books, 2014.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Kindle edition. Oxford University Press, 2013.

Sulmeyer, Michael. "Study Group: Problem Solving in Cyberspace Operations." Harvard University Kennedy School of Government, February 2016.

Summerfield, Penny. "Gender and War in the Twentieth Century." *The International History Review* 19, no. 1 (March 1997): 3–15. doi:10.1080/07075332.1997.9640771.

Switala, Kristin. "The Feminist Theory Website: English Introduction." Accessed February 8, 2016. http://www.cddc.vt.edu/feminism/enin.html.

Terry, ed., Jennifer, and Melodie Calvert, ed. *Processed Lives: Gender and Technology in Everyday Life*. Psychology Press, 1997.

The Economist. *Richard A. Clarke: Cyberwar in 2013*. Video Interview, 2012. https://www.youtube.com/watch?v=6_ek8mugOUc.

"Thesis on Cyber War - Seeking Advice on Resources," January 2016. https://mail.google.com/mail/u/0/#search/reveron/15236ade57b2e196.

Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies* 27, no. 1 (January 2, 2014): 101–30. doi:10.1080/13518046.2014.874845.

Tighe, Jan. "Vice Admiral Tighe's Letter to the Information Warrior Community.pdf," February 12, 2016. http://www.public.navy.mil/fcc-c10f/Pages/home.aspx.

Turkle, Sherry. “The Flight From Conversation.” *The New York Times*, April 21, 2012. http://www.nytimes.com/2012/04/22/opinion/sunday/the-flight-from-conversation.html.

Turkle, Sherry, and Cheris Kramarae, ed. “Computational Reticence: Why Women Fear the Intimate Machine.” In *Technology and Women’s Voices: Keeping in Touch*, 33–49. Routledge, 1988.

Tuutti, Camille. “National Security Agency Celebrates Diversity, Introverts -- FCW.” *FCW: The Business of Federal Technology - Circuit*, April 16, 2012. https://fcw.com/blogs/circuit/2012/04/fedsmc-chris-inglis-federal-workforce.aspx.

United States Department of Defense. *The Making of a Cyber Warrior - DoD News*. Youtube Video, 2013. https://www.youtube.com/watch?v=WbmTqzLHBGA.

United States Navy. “Information Dominance Corps.” *United States Naval Academy Center for Cyber Security Studies*. Accessed February 15, 2016. http://www.usna.edu/CyberCenter//_files/documents/idc/IDC_Overview.pdf.

“(U) NSA Culture, 1980s to the 21st Century--a SID Perspective.” Accessed February 19, 2016. https://www.nsa.gov/public_info/_files/cryptologic_quarterly/NSA_Culture.pdf.

“USA QuickFacts from the US Census Bureau.” *United States Census Bureau*. Accessed February 21, 2016. http://quickfacts.census.gov/qfd/states/00000.html.

“U.S. Cyber Command - U.S. Strategic Command.” Accessed January 17, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

“U.S. Federal Cybersecurity Operations Team: National Roles and Responsibilities,” March 5, 2013. http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/2013march21_cyberroleschart.authcheckdam.pdf.

Wajcman, Judy. “Technocapitalism Meets Technofeminism: Women and Technology in a Wireless World.” *Labour & Industry* 16, no. 3 (May 2006): 7–20.

Williamson, Murray. “Military Culture Does Matter.” Foreign Policy Research Institute, June 2012. http://www.fpri.org/article/2012/06/military-culture-does-matter/.

“Women and Information Technology By the Numbers.” *National Center for Women & Information Technology*, February 28, 2014. http://www.ncwit.org/sites/default/files/resources/btn_02282014web.pdf.

Zekany, Eva. “The Gendered Geek: Performing Masculinities in Cyberspace.” Central European University, Department of Gender Studies, 2011.