Security Studies

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fsst20

Masculinist Actionism: Gender and Strategic Change in US Cyber Strategy

Katharine M. Millar & James Shires

To cite this article: Katharine M. Millar & James Shires (11 Jun 2024): Masculinist Actionism: Gender and Strategic Change in US Cyber Strategy, Security Studies, DOI: 10.1080/09636412.2024.2351918

To link to this article: https://doi.org/10.1080/09636412.2024.2351918

Published online: 11 Jun 2024.

SECURITY STUDIES
https://doi.org/10.1080/09636412.2024.2351918

Routledge
Taylor & Francis Group

Masculinist Actionism: Gender and Strategic Change in US Cyber Strategy

Katharine M. Millar and James Shires

ABSTRACT

How do gender hierarchies inform processes of strategic change? Drawing upon feminist institutionalism and security studies, we argue that gender hierarchies form the boundaries of acceptability for strategic change. We conduct a qualitative feminist analysis of cyber strategy policy documents and expert commentary around a 2018 shift in US cyber strategy. We identify two ideal-typical modes of masculinity—military and "tech"—as influential in conditioning US cyber strategy. The interaction of these masculinities facilitated the emergence of "defending forward" and "persistent engagement" as proactive, dynamic, and suitably masculine new strategic concepts. The previously preferred strategic concept, deterrence, conversely, was constructed in line with feminized tropes as weak, passive, and reactive. Strategic change is facilitated by a change in the meaning of a specific gender norm—masculinized action—while still constrained by the continuation of a broader gender hierarchy of masculinities over femininities, and the associated valorization of action over passivity and dependence.

How do gender hierarchies inform processes of strategic change? This article draws upon the insights of feminist institutionalism and feminist security studies to argue that gender, as expressed in social structures and intersubjective ideas, beliefs, norms, and expectations, shapes strategic change processes.[1] By this, we do not mean that gender directly causes specific policies to be discarded and adopted. Instead, it constitutes the parameters within which strategic debates occur and candidate concepts emerge.[2] More specifically, we argue that a hierarchical valorization of concepts, symbols, and actions associated with masculinity and denigration of ideals associated with femininity constrains the "acceptability" of

Katharine M. Millar is an Associate Professor in the Department of International Relations at the London School of Economics. Her research examines the gendered, sexualised, and racialised politics of violence.
James Shires was formerly an Assistant Professor in Cybersecurity Governance at the University of Leiden. He is now the Co-Director of the European Cyber Conflict Research Initiative (ECCRI).

[1]Laura Sjoberg, "Introduction to Security Studies: Feminist Contributions," *Security Studies* 18, no. 2 (2009): 187; Kimberly Hutchings, "Making Sense of Masculinity and War," *Men and Masculinities* 10, no. 4 (2008): 389–404.

[2]Alexander Wendt, "On Constitution and Causation in International Relations," *Review of International Studies* 24, no. 5 (1998): 101–18.

candidate strategic concepts.[3] Contextual changes in the meaning of specific gender norms—particularly masculinized expectations of action—facilitate strategic shifts that nonetheless align with broader gender hierarchies.

We make this argument through an examination of US cyber strategy. As a comparatively recent field, cyber strategy is characterized by contestations over conceptual meanings, strategic goals, and practices that surface otherwise implicit or sedimented gendered logic. We analyze a notable 2018 shift in US cyber strategy, away from ideas of "deterrence" toward new concepts of "persistent engagement" and "defending forward" in two steps.

First, although Cold War military discourse constructed deterrence as valorized protective action, aligning with gendered expectations of military masculinity, in cyber strategy, deterrence came to be negatively associated with a feminized acceptance of pervasive, low-level vulnerability.[4]

Second, at the same time, ideals of masculinity shifted in the broader United States, Department of Defense, and armed forces. Classical military conceptions of masculinity came to interact with masculine ideals associated with the rise of "big tech," such as individualism, problem-solving, and technological competence. These simultaneous shifts—in the gendered devalorization of a strategic concept (deterrence) and the kind of activities associated with masculinity—contributed to the emergence of "persistent engagement" and "defend forward" as acceptable strategic alternatives. Although differing in their understanding of what counts as action, these distinct masculine ideals share a commitment to "doing something" present throughout Western gender hierarchies, which we refer to as "masculinist actionism."[5]

This article makes two contributions to security studies. First, the article establishes that gender hierarchies constitute the boundaries of acceptability for strategic change. Feminist security studies has examined the relationship between gender and the military in detail.[6] Less work, however, has examined the role of gender in state strategy, as the vision for how "military instruments *per se* are to achieve the goals set for them."[7] Scholarship

[3]Mimi Schippers, "Recovering the Feminine Other: Masculinity, Femininity, and Gender Hegemony," *Theory and Society* 36, no. 1 (2007): 85–102; Lauren Wilcox, "Gendering the Cult of the Offensive," *Security Studies* 18, no. 2 (2009): 219–20; Eric M. Blanchard, "Gender, International Relations, and the Development of Feminist Security Theory," *Signs* 28, no. 4 (2003): 1289–312; Sjoberg, "Feminist Contributions."

[4]Carol Cohn, "Sex and Death in the Rational World of Defense Intellectuals," *Signs* 12, no. 4 (1987): 687–718.

[5]The term "actionism" was coined by Brent Steele, in *Restraint in International Politics* (Cambridge: Cambridge University Press, 2019).

[6]See, for instance: Claire Duncanson, "Forces for Good? Narratives of Military Masculinity in Peacekeeping Operations," *International Feminist Journal of Politics* 11, no. 1 (2009): 63–80; Anthony King, "Women in Combat," *The RUSI Journal* 158, no. 1 (2013): 4–11.

[7]Stephen Biddle, "Strategy in War," *PS: Political Science & Politics* 40, no. 3 (2007): 461–2. For exceptions, see: Claire Duncanson and Catherine Eschle, "Gender and the Nuclear Weapons State: A Feminist Critique of the UK Government's White Paper on Trident," *New Political Science* 30, no. 4 (2008): 545–63; Cohn, "Sex and Death"; Wilcox, "Cult of the Offensive."

examining how gender informs military outcomes considers primarily the tactical and operational levels.[8] Second, although there is literature examining women's participation in cybersecurity as a professional field and, separately, the gendered effects of cyber operations, this is the first study to interrogate the way gender constitutes cyber strategic concepts, logics, and assumptions.[9]

The article begins by outlining how gender helps to understand the role of power in (cyber) strategy. Second, we give a feminist institutionalist account of how gender constitutes strategic change. Next, we summarize our methodology: qualitative feminist analysis of US cyber strategic policy documents and debates. The fourth section provides an empirical analysis of the feminization of cyber deterrence during the Obama administration and, subsequently, the masculinization and adoption of persistent engagement and defend forward during the Trump administration. The conclusion connects this strategic change to the wider logic of masculinist actionism, concluding with theoretical and policy implications.

Strategic Change and Cyber Strategy

The digital age is not the first time new technologies have accompanied strategic revision. Examining cyber strategy as a case of general strategic change avoids fixating on technological innovation and proliferation.[10] During strategic change, multiple strategies co-exist and compete until they are accepted or discarded, usually through cumulative pressures of bureaucratic politics and ideational revision where, we argue, gender acts as a constitutive condition bounding the acceptability of different strategic concepts.

Over the last two decades, many states have developed dedicated cyber strategies to counter a range of new digital threats, including from other states. States increasingly recognize cyber operations as a core instrument

[8]For example, see: Keally McBride and Annick Wibben, "The Gendering of Counterinsurgency in Afghanistan," *Humanity* 3, no. 2 (2012): 199–215; Heidi Hardt and Stéfanie von Hlatky, "NATO's About-Face: Adaptation to Gender Mainstreaming in an Alliance Setting," *Journal of Global Security Studies* 5, no. 1 (2020): 136–59.

[9]For women's participation in cybersecurity, see: Donna Peacock and Alistair Irons, "Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression," *International Journal of Gender, Science, and Technology* 9, no. 1 (2017): 25–44. For gendered effects of cyber operations, see: Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security," *Association for Progressive Communications*, April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. On the necessity of this analysis, see: Salma Shaheen, "Offense–Defense Balance in Cyber Warfare," in *Cyberspace and International Relations,* ed. J.-F. Kremer and B. Müller (Berlin: Springer, 2014): 77–93. For an analysis of cybersecurity and masculinity in general, see: Joseph Da Silva, "Protection, Expertise and Domination: Cyber Masculinity in Practice," *Computers & Security* 133 (2023).

[10]David Edgerton, *The Shock of the Old: Technology and Global History Since 1900* (London: Profile Books, 2007); Scott D. Sagan, "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb," *International Security* 21, no. 3 (1996): 54–86. Technological inferiority may accompany strategic success, as common in counterinsurgency. See: Jon R. Lindsay, *Information Technology and Military Power* (Ithaca: Cornell University Press, 2020).

of national power, a judgment reflected in the proliferation of the capabilities themselves (which are difficult to develop and maintain) and in the discourse around them—including assessments of relative levels of "cyber power" between states.[11] While most states still do not acknowledge the existence of their offensive cyber capabilities, this is changing rapidly. Many, including the United States, have established cyber structures in their militaries. The US Cyber Command was founded in 2009, well before many other states began investing in this area. Debates regarding the appropriate use of cyber capabilities in the United States trace back at least to the 1990s Revolution in Military Affairs.[12]

The United States has a track record of cyber operations, including the infamous Stuxnet virus targeting Iranian nuclear enrichment facilities, discovered in 2010 and widely believed to usher in a new era of "cyber war."[13] In the subsequent decade, US cyber strategy grew to include a wide range of espionage campaigns and disruptive operations. Many of these operations surfaced in the public domain after being tracked by cybersecurity companies or revealed by the leaking of documents or the cyber tools themselves. The United States has acknowledged Cyber Command deployments against adversaries such as Iran and Russia and in combat situations such as the coalition campaign against ISIS in Syria and Iraq.[14]

Despite its use of sophisticated offensive cyber capabilities, however, an increasing number of high-profile cyber operations by other states have contributed to an assessment of the United States as consistently on the back foot. Many operations, such as Iranian "wiper" attacks in the Gulf since 2012 or the 2017 North Korean and Russian repurposing of US exploits to cause worldwide digital chaos, indirectly affected the United States through their allies or the global economy. Others, such as Iranian "denial-of-service" attacks against the US financial sector in 2012–13, Chinese infiltration of the Office of Personnel Management (OPM) in 2015, and 2016 Russian election interference, targeted the United States directly. These incidents led to soul-searching by US cyber strategists, with

[11]Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022); Julia Voo et al., "National Cyber Power Index 2020," *Belfer Center*, September 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf; International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," *International Institute for Strategic Studies*, June 28, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[12]John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington, DC: RAND, 1997); David V. Gioe, Michael S. Goodman, and Tim Stevens, "Intelligence in the Cyber Era: Evolution or Revolution?," *Political Science Quarterly* 135, no. 2 (2020): 191–224.

[13]Kim Zetter, *Countdown to Zero Day* (New York: Penguin Random House, 2014); David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018).

[14]Michael Sexton and Eliza Campbell, eds., *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization* (Washington, DC: Middle East Institute, 2020); Julian Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

the Obama administration's clumsy attribution and inconsistent response after North Korea dismantled the networks of Sony Pictures Entertainment in 2015 demonstrating deep strategic confusion.[15] The 2018 shift in US cyber strategy was thus motivated by innovation from its adversaries and a perceived failure to respond adequately. This shift also occurred within a changing US foreign policy, shifting commitments in the Middle East, and rising great power competition from peer adversaries, especially over advanced technologies.

Within the cybersecurity literature, influential accounts of the 2018 shift focus on the interplay between technology and strategy.[16] These accounts argue that the United States failed to capitalize upon the revolutionary implications of digital technologies to the extent that adversary cyber operations were a better "fit" to the technological environment.[17] Further explanations highlight bureaucratic politics and inter-agency competition regarding institutional ownership of intelligence capabilities.[18]

Others emphasize ideational factors in shaping US cyber strategy.[19] Such works highlight the influence of military culture—and contextual notions of prestige, authority, and legitimacy—on US cyber strategy, including the 2018 shift itself.[20] These accounts, however, include limited consideration of the baseline analytical concepts themselves.[21] Lonergan and Schneider

[15]Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, (Cambridge, MA: Harvard University Press, 2020).

[16]Joseph Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48; Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* 45, no. 4 (2022): 534–67.

[17]Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017); Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies* 42, no. 6 (2019): 841–63; Richard J. Harknett, "SolarWinds: The Need for Persistent Engagement," *Lawfare*, December 23, 2020, https://www.lawfareblog.com/solarwinds-need-persistent-engagement.

[18]Steven Loleski, "From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations to Shadow Brokers," *Intelligence and National Security* 34, no. 1 (2019): 112–28; Stefan Soesanto, "The Evolution of US Defense Strategy in Cyberspace (1988 – 2019)," *CSS Cyberdefense Trend Analyses,* August 28, 2019, https://www.research-collection.ethz.ch/handle/20.500.11850/366192; Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem." *Intelligence and National Security* 36, no. 2 (2021): 260–78.

[19]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics* (London: Routledge, 2008); David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: International Institute for Strategic Studies, 2011).

[20]Sarah White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine," PhD diss., Harvard University, 2019: 9; Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD," *The Cyber Defense Review* 5, no. 2 (2020); Rebecca Slayton, "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018," *Texas National Security Review* 4, no. 1 (2021): 62–96. For the 2018 shift, see: Erica D. Lonergan and Jacquelyn Schneider, "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation," *Journal of Cybersecurity* 9, no. 1 (2023).

[21]Exceptions include: Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization* 75, no. 1 (2021): 1–32; Rebecca Slayton, "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018," *Texas National Security Review* 4, no. 1, (2021): 62–96; Rebecca Slayton, "(De)Stabilizing Cyber Warriors: The Emergence of US Cyber Expertise, 1967-2008," in *Cyberspace and Instability*, ed. James Shires, Robert Chesney, and Max Smeets (Edinburgh: Edinburgh University Press, 2023): 177–216.

attribute the 2018 shift to changes in policymakers' beliefs around norms, deterrence, and the risks of escalation, but without accounting for the social, ideational, and relational processes generating—and limiting—such changes in belief.[22] Branch's account of how foundational metaphors draw the bounds of strategic contestation does not sufficiently interrogate why certain metaphors "succeed" in becoming commonsense.[23]

The cyber strategy literature, paralleling the strategic studies literature, sidesteps the deeper construction of concepts such as legitimacy, expertise, and commonsense and, vitally, their embedding in power relations. Feminist theories challenge the "found" meanings of these core concepts, arguing that, as intersubjective ideas located in specific socio-cultural contexts, they reflect and reproduce a series of gendered assumptions about power, agency, hierarchy, and overall worldview.[24] The (cyber) strategy literature's failure to engage with gender, as both a "constitutive element of social relationships… and a primary way of signifying relationships of power," thus limits its ability to account for the role of power in producing strategic commonsense.[25]

This omission occurs despite empirical indications that gendered hierarchies operate in US cyber strategy. White, for instance, traces the origins of cyber operators in the Navy to pre-1995 restrictions on women in combat and the related formation of the shore-based General Unrestricted Line Community (GURL), who specialized in electronic communications.[26] The indirectly demeaning, gendered name of the group is indicative of a gendered hierarchy within naval occupations, with electronic communications placed below conventional roles. Similarly, studies of NSA code names for different stages of a cyber operation—including BLINDDATE, HAPPYHOUR, NIGHTSTAND, and SECONDDATE, culminating in PANT_SPARTY—suggest that in the United States at least, "sexual exploitation is an official metaphor of [cyber] operations."[27]

The cyber strategy literature thus mirrors a broader trend in strategic studies, wherein, despite general agreement that the question of "fit" between strategy and technology is as much a social question as a functional one, the role of gender as constitutive of this "fit"—in making strategic change acceptable—is overlooked.[28] Strategy does not change

[22]Lonergan and Schneider "Power of Beliefs," 4.

[23]Branch, "Metaphors and Cybersecurity."

[24]Laura Sjoberg, *Gender, War, and Conflict* (New York: John Wiley & Sons, 2014); Sandra Harding, "Rethinking Standpoint Epistemology: What Is "Strong Objectivity?," *The Centennial Review* 36, no. 3 (1992): 437–70.

[25]Joan W. Scott, "Gender: A Useful Category of Historical Analysis," *American Historical Review* 91, no. 5 (1986): 1067, as cited in Mary Hawkesworth, "Engendering Political Science: An Immodest Proposal," *Politics & Gender* 1, no.1 (2005): 143.

[26]White, "Subcultural Influence," 312.

[27]Barton Gellman, *Dark Mirror: Edward Snowden and the Surveillance State* (London: Bodley Head, 2020).

[28]Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge: MIT Press, 1978); Geoffrey L. Herrera, *Technology and International Transformation: The*

simply as a direct reflection of material change, objective strategic need, environmental mismatch or, indeed, instrumentally rational assessment, but also as a reflection of social, ideational and institutional power. This operation of this power, in turn, cannot be understood without attending to gender. As such, our argument is best understood not as an alternative causal explanation of strategic change but as a complement to existing accounts. We foreground gendered hierarchies as an analytically overlooked constitutive component of broader strategic change processes.

More specifically, as we detail in the following sections, gender matters because it tells us about the role of power in drawing the boundaries of acceptable strategic change. Gender hierarchies reflect and reinforce power relations across society, government, and the national security establishment that inform which (cyber) strategy concepts appear acceptable and commonsensical.

Conceptual Framework: Gender and Strategic Change

In this section, we develop a feminist institutionalist framework for understanding the relationship between gender and strategic change. We argue that strategic commonsense is constituted within a gendered hierarchy that valorizes masculinized concepts, ideas, and practices over feminized ones, thus setting the general parameters within which strategy is evaluated as legitimate, authoritative, viable, and so on. Shifts in the contextual meaning of specific gender norms alter the acceptable boundaries of strategic change—centrally, the masculinist expectation of "action"—that nonetheless continue to align with an overarching gender hierarchy privileging masculinity over femininity.

Broadly, feminist institutionalism argues that institutions shape gendered identities, norms, beliefs, and practices and are, in turn, shaped by gendered assumptions and practices articulated within the institution but informed by broader society.[29] Gender is related to, but exceeds, embodied identity and bodily performance. It is also a set of intersubjective beliefs, values, characteristics, attributes, expectations, and conceptual associations that act as a normative social structure.[30]

Consequently, as argued by Kronsell, organizations tend to have "particular 'pattern-bound' effects over time," created by the entrenchment of

Railroad, the Atom Bomb, and the Politics of Technological Change (Albany: State University of New York Press, 2007).

[29]Joan Acker, "Hierarchies, Jobs, Bodies: A Theory of Gendered Organizations," *Gender & Society* 4, no. 2 (1990): 139-158; Fiona Mackay, Meryl Kenny, and Louise Chappell, "New Institutionalism Through a Gender Lens: Towards a Feminist Institutionalism?," *International Political Science Review* 31, no. 5 (2010): 573–88.

[30]Although often understood as expressing expectations for men and women, gender is non-binary and diverse.

informal rules and norms of behavior which are themselves gendered.[31] These hierarchical gendered expectations and norms related to the meaning of legitimacy, authority, and expertise come to be institutionally internalized as a form of commonsense.[32] They are the background against which policy ideas are evaluated, constituting the institutional "conditions for action that can make a certain course of action more or less appropriate or promising."[33] For specific institutional actors—in our case, cyber policymakers from across the US government and associated expert commentators—this institutional context reproduces a "gendered logic of appropriateness" that implicitly or explicitly outlines the expectations for "'acceptable' masculine and feminine forms of behaviour, rules, and values."[34] Gendered hierarchies are thus an important dimension of intersubjective power that both enable and constrain action.

For feminist institutionalism, gendered structures and norms constitute even social and institutional contexts that do not have significant embodied gender diversity (and are predominantly staffed by people identifying as men), including national security and information technology.[35] Likewise, shifts in gendered institutional norms, practices, and hierarchies need not be a move between binary concepts of masculinity and femininity, or from a "gendered" policy to an imagined "gender neutral" alternative. Shifts between modes of masculinity (or femininity) and contestations over contextually valorized masculinity, also inform broader shifts in institutional power.[36]

In the balance of this section, we draw upon feminist security and feminist science and technology studies to identify two forms of idealized masculinity—military and "tech" masculinities—that constitute the parameters for what "counts" as legitimate, authoritative, and prestigious and, in turn, what can be constructed as viable, active cyber strategic change.

Feminist security studies establish the relevance of socially embedded gendered institutions and organizational cultures to strategy. In Wilcox's examination of the paradoxical persistence of the "cult of the offensive" in pre-World War One Europe, she argues that military masculinity—gender norms associated with soldiering, such as bravery, aggression, sacrifice,

[31]Annica Kronsell, "Sexed Bodies and Military Masculinities: Gender Path Dependence in EU's Common Security and Defense Policy," *Men and Masculinities* 19, no. 3 (2016): 315–6.

[32]Raewyn Connell, *Gender* (Cambridge: Polity Press, 2002); Kronsell, "Sexed Bodies," 316.

[33]Teresa Kulawik, "Staking the Frame of a Feminist Discursive Institutionalism," *Politics & Gender* 5, no. 2 (2009): 262–71.

[34]Louise Chappell and Georgina Waylen, "Gender and the Hidden Life of Institutions," *Public Administration* 91, no. 3 (2013): 599–615.

[35]Susan Marlow and Angela Martinez Dy, "Annual Review Article: Is it Time to Rethink the Gender Agenda in Entrepreneurship Research?," *International Small Business Journal* 36, no. 1 (2018): 3–22.

[36]Claire Duncanson, "Hegemonic Masculinity and the Possibility of Change in Gender Relations," *Men and Masculinities* 18, no. 2 (2015): 231–48.

violence, and physical strength—constituted pre-WWI strategic culture.[37] This led to a misperception of the technological offense-defense balance, facilitated by a gendered ideology of national "protection" that legitimated (and necessitated) violent military action, and resulted in a preference for aggressive strategic concepts.[38] Slayton identifies a similar misperception—that cyberspace favors offense—as characterizing early US cyber strategy, to the point of likewise forming a "cult of the offensive."[39]

Military masculinity constitutes national security via a gendered logic of protection. More specifically, discourses of military masculinity construct the state as protecting the vulnerable citizenry, demonstrating ideally masculine characteristics of autonomy, public service, and self-sacrifice.[40] They present the military as protecting a weaker, but normatively valued, feminized civilian sphere.[41] In military institutions, this manifests in a gendered hierarchy of masculine prestige, which valorizes infantry occupations and practices over non-combat roles.[42] Masculinized violence (even death), rather than feminized forbearance and/or suffering, is the benchmark for politically-acceptable security strategy.[43] This "warrior model" of masculinity, which implicitly valorizes offensive strategic concepts over defensive, informs a contextual preference for masculinized/ising *action* that characterizes national security overall.[44]

The appeal of military masculinity extends beyond the armed forces. Broader US (and Western) society regard military masculinity and its characteristics as desirable, laudable, and status-conferring.[45] This can be seen in everything from the popularity of military-related video games such as *Call of Duty* to the valorization of military personnel at US sporting events.[46] Military service is an electoral asset for US politicians; women encounter gendered stereotypes in seeking to exercise defense-policy leadership.[47]

[37]Katharine Millar and Joanna Tidy, "Combat as a Moving Target: Masculinities, the Heroic Soldier Myth, and Normative Martial Violence," *Critical Military Studies* 3, no. 2 (2017): 142–60; Wilcox, "Cult of the Offensive."

[38]Wilcox, "Cult of the Offensive"; Iris Marion Young, "The Logic of Masculinist Protection: Reflections on the Current Security State," *Signs* 29, no. 1 (2003): 1–25.

[39]Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2016): 72–3.

[40]Young, "Gendered Logic of Protection," 9.

[41]Jean Bethke Elshtain, *Women and War* (Chicago: University of Chicago Press, 1995).

[42]Joanna Tidy, "The Gender Politics of "Ground Truth" in the Military Dissent Movement: The Power and Limits of Authenticity Claims regarding War," *International Political Sociology* 10, no. 2 (2016): 99–114.

[43]Veena Das, "Violence, Gender, and Subjectivity," *Annual Review of Anthropology* 37 (2008): 283–99.

[44]Wilcox, "Cult of the Offensive," 227.

[45]Katharine Millar, "What Do We Do Now? Examining Civilian Masculinity/Ies in Contemporary Liberal Civil-Military Relations," *Review of International Studies* 45, no. 2 (2019): 239–59.

[46]Frédérick Gagnon, "Invading Your Hearts and Minds": Call of Duty® and the (Re) Writing of Militarism in US Digital Games and Popular Culture," *European Journal of American Studies* 5, no. 5–3 (2010): 1–20; Michael Butterworth and Stormi Moskal, "American Football, Flags, and "Fun": The Bell Helicopter Armed Forces Bowl and the Rhetorical Production of Militarism," *Communication, Culture & Critique* 2, no. 4 (2009): 411–33.

[47]Michele Swers, "Building a Reputation on National Security: The Impact of Stereotypes related to Gender and Military Experience," *Legislative Studies Quarterly* 32, no. 4 (2007): 559–95.

Military masculinity is not, however, the sole model for idealized "manliness" in the contemporary United States; masculinities (and femininities) are plural and changeable.[48] Across the twentieth century, gender scholars document a transformation, spurred by economic globalization, in the attributes associated with "idealized" US masculinity.[49] These characteristics shifted away from those associated with blue-collar occupations, such as manual labor and "hard work," toward those associated with white-collar jobs, such as interpersonal skills, flexibility, and entrepreneurialism.[50]

This transition in gender norms contextualized the rise, beginning in approximately 1980, of technology-intensive fields such as computing and cybersecurity.[51] Gender norms construct technology in general, including its change over time.[52] As a function of these transformations in masculinities—and men's greater access to opportunities to develop technical skills—US and similar societies associate technical expertise and competence with masculinity.[53] Supposed masculine attributes include dominance "over the machine" (and those with less technical competence).[54] This means that "engineering culture, with its fascination with computers and the most automated techniques, is archetypically [if not essentially] masculine."[55]

More recently, as observed by Dunbar-Hester, "programmers, computing magnates and hackers have catapulted into the limelight," as founders are upheld as aspirational geniuses of technical skill and business acumen.[56] The dot-com boom and rise of startup culture within Silicon Valley facilitated a revision in the meaning of the "computer geek."[57] In contrast to the "nerd," who is simply "uncool," the geek embodies valued attributes such as technical mastery, innovation, and risk-taking that also characterize heroic masculine agency.[58]

[48]Raewyn Connell and James W. Messerschmidt, "Hegemonic Masculinity: Rethinking the Concept," *Gender & Society* 19, no. 6 (2005): 829–59.

[49]Sunera Thobani, "Vigilante Masculinity and the 'War on Terror'," in *Islam in the Eyes of the West: Images and Realities in an Age of Terror*, ed. Tareq Y. Ismael and Andrew Rippin (London: Routledge, 2010): 64–85.

[50]Charlotte Hooper, *Manly States: Masculinities, International Relations, and Gender Politics* (New York: Columbia University Press, 2001), 156–7.

[51]Christina Dunbar-Hester, *Hacking Diversity: The Politics of Inclusion in Open Technology Cultures* (Princeton: Princeton University Press, 2020), 35.

[52]Cynthia Cockburn, "The Circuit of Technology: Gender, Identity and Power," in *Consuming Technologies: Media and Information in Domestic Spaces*, ed. Eric Hirsch and Roger Silverstone (London: Routledge, 2003), 33–42.

[53]Cynthia Cockburn, "On the Machinery of Dominance: Women, Men, and Technical Know-How," *Women's Studies Quarterly* 37, no. 1/2 (2009): 269–73.

[54]Judy Wajcman, *Feminism Confronts Technology* (Pittsburgh: Penn State Press, 1991), 144.

[55]Wajcman, *Feminism Confronts Technology*, 48.

[56]Dunbar-Hester, *Hacking Diversity*, 35; Nathan Ensmenger, *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise* (Cambridge: MIT Press, 2012).

[57]Nathan Ensmenger, ""Beards, Sandals, and Other Signs of Rugged Individualism": Masculine Culture within the Computing Professions," *Osiris* 30, no. 1 (2015): 38–65.

[58]Wajcman, *Feminism Confronts Technology*, 144; Alison Adam, *Gender, Ethics and Information Technology* (London: Palgrave Macmillan, 2005). Within popular culture, geeks remain inflected by ideas of physical weakness, antisocial tendencies, and "outsider" status. Dunbar-Hester, *Hacking Diversity,* 33.

The contemporary understanding (if not practice) of hacking also informs this shift in masculinity.[59] Hacking, for Turkle, embodies masculine values of mastery, domination, and control, suggesting that "though hackers would deny that theirs is a macho culture, the preoccupation with winning and of subjecting oneself to increasingly violent tests would make their world peculiarly male in spirit."[60] Hacking also draws on neoliberal entrepreneurialism: individualism, rule-breaking, and a disdain for bureaucratic hierarchies and institutional procedures.[61]

This cultural milieu prizes the ability to produce "innovative" technological solutions to problems above all else.[62] In Dunbar-Hester's terms, this is an attitude of an "alpha geek competitive masculinity."[63] Such solutionism frequently involves disregarding institutional, legal, and social norms, enabling unequal and problematic gendered (and sexualized, classed, racialized, etc.) practices in many tech environments.[64] Media and professional discourses also construct this form of idealized masculinity as White and (upper)middle class, through racialized and gendered logics that contrast the "genius" technologist with the more routinized and banal work of the feminized "coder"—a trope projected upon Asian Americans and other minoritized groups.[65]

The valorization of military masculinity in the contemporary United States thus exists alongside an emergent form of idealized masculinity that combines elements of "geek"/computing masculinities with the neoliberal, "genius" sensibilities of startup capitalism.[66] We refer to this archetype as "tech" masculinity.[67]

The substantive characteristics of these two ideal-typical forms of masculinity—military and "tech"—are sketched in Table 1.

We express the two forms of masculinity in separate rows, although they are not hermetically sealed. People and institutions involved in

[59]"Hacker" has a long history of queer and ambivalent identities and dynamics. Leonie Tanczer, "Hacktivism and the Male-Only Stereotype," *New Media & Society* 18, no. 8 (2016): 1599–615.

[60]*Wajcman, Feminism Confronts Technology*, 141–2; Marianne Cooper, ""Being the "Go-To Guy": Fatherhood, Masculinity, and the Organization of Work in Silicon Valley," *Qualitative sociology* 23 (2000): 379–405.

[61]Heather Mendick et al., "Geek Entrepreneurs: The Social Network, Iron Man and the Reconfiguration of Hegemonic Masculinity," *Journal of Gender Studies* 32, no. 3 (2023): 283–95; Emily Crandall, Rachel Brown, and John McMahon, "Magicians of the Twenty-First Century: Enchantment, Domination, and the Politics of Work in Silicon Valley," *Theory & Event* 24, no. 3 (2021): 841–73.

[62]Cooper, "Go-to Guy."

[63]Dunbar-Hester, *Hacking Diversity,* 201.

[64]Emily Chang, *Brotopia: Breaking Up the Boys' Club of Silicon Valley* (Portfolio, 2019).

[65]Dunbar-Hester *Hacking Diversity,* 36–7; Ensmenger, "Rugged Individualism," 65; Safiya Noble and Sarah Roberts, "Technological Elites, the Meritocracy, and Postracial Myths in Silicon Valley," *Racism Postrace Report #6* 2019, https://escholarship.org/uc/item/7z3629nh; Tiffany Y Chow, "Privileged but Not in Power: How Asian American Tech Workers Use Racial Strategies to Deflect and Confront Race and Racism," *Qualitative Sociology* 46, no. 1 (2023): 129–52.

[66]Mendick et al., "Geek Entrepreneurs."

[67]The use of "tech" to stand for digital technologies alone is simplistic, but follows common usage (e.g., "big tech").

strategic construction and contestation draw upon, and are bound by, multiple gendered logics.

Military and tech masculinities share an investment in the values of idealized Western masculinity: rationality, autonomy, and control.[69] The gendered construction of autonomy and control as masculine results in the construction of agency itself as masculine.[70] Likewise, each form of masculinity draws contrasts with not only other forms of masculinity, but also concepts, ideals, and values associated with women, femininity, and/or queerness, seen as denigrated and/or inferior.[71] These commonalities manifest in a strategically important commitment to *action* and aversion to frequently feminized concepts such as vulnerability, dependence, and passivity.

Both modes of masculinity are embedded within a broader gender hierarchy that valorizes masculinities over femininities and action over passivity/dependence. However, the existence and contestation of multiple valorized forms of masculinity means that the *meaning* of action differs across military and tech masculinities. This shift in the contextual gendered expectations of masculinity alters the boundaries of acceptable strategic change while still preserving a broader gendered hierarchy of masculinities over femininities.

Methodology

Methodologically, we conduct a qualitative gender analysis, informed by feminist institutionalism, of policy documents, public commentary, and

Table 1. Schematic summary of ideal-typical masculinities.[68]

Ideal-type masculinity	Key elements	Gendered logic of action	Strategic consequences	Manifestation in cyber strategy
Military	Bravery, aggression, sacrifice, violence, physical strength	State protects society	Denigration of defense, "cult of the offensive"	Deterrence and superiority in armed conflict; inaction below threshold of "war"
Tech	Technical mastery, innovation, autonomy, risk-taking	Engineers solve for consumers	Valorization of defense, autonomous risk-taking	Defend forward and persistent engagement; constant action to counter adversaries

[68]These logics of masculinity exist in conversation with relations of sexuality, class, race, ability, and age – important avenues for future work.

[69]Elisabeth Prügl, "Feminism and the Postmodern State: Gender Mainstreaming in European Rural Development," *Signs* 35, no. 2 (2010): 454–5.

[70]See: William Waller and Mary V. Wrenn, "Feminist Institutionalism and Neoliberalism," *Feminist Economics* 27, no. 3 (2021): 51–76.

[71]Lori Kendall, *Hanging Out in the Virtual Pub: Masculinities and Relationships Online* (Berkeley: University of California Press, 2002), 87; Aaron Belkin, *Bring Me Men: Military Masculinity and the Benign Façade of American Empire* (New York: Hurst, 2012).

media reporting to interrogate the gender norms and dynamics relevant to US cyber strategy. We examine these texts for their expression of key gendered elements that enable us to trace the interaction of military and tech masculinities in constituting strategic change.

We understand these three closely connected types of sources as representing different angles on the shared vernacular, institutional cultures, and gendered norms and assumptions of the broader cyber strategy community that circulates between thinktank commentary, the academy, and US government policy. These texts are "public" in the sense that they are freely available, but their main producers and consumers are expert cyber security practitioners/policymakers. We do not view the texts as wholly independent articulations of either cyber strategy or gender norms; instead, we approach them as a shared strategic and institutional space that uses different forms of communication about similar ideas. (See the Appendix for the full document list.)[72]

We are interested less in the intention behind the inclusion of specific words within a given policy document than the gendered logics and negotiations that language reveals and constructs.[73] Likewise, we are attentive to the fact that a contextual process of association and contrast with other ideas, concepts, and values leads to the gendering of assumptions, hierarchies, and dynamics—including those pertaining to "action."[74] We, therefore, use the documents, read in their entirety, to assess the production and operation of gender within US cyber strategy. Analytically, we move from an examination of *implicit* gendered assumptions and logic found within formal cyber strategy documents to more *explicit* statements of institutional gendered expectations, identities, and hierarchies within expert commentary and media reporting. We then illustrate these gender dynamics through representative quotations that succinctly convey broader patterns of gendered strategic constitution.

Concretely, we first examine all cyber strategy documents produced by the Department of Defense, the National Security Council, Cyber Command, and other policy or legislative bodies between 2001 and 2021, with particular attention to the 2018 strategic shift. We use only those documents that centrally refer to cyber strategy rather than broader security, intelligence, or defense strategies that include references to cyber matters.[75] Few of these documents directly mention gender, men, or women. We would not expect them to. Most national security documents do not explicitly

[72]Katharine Millar, "Appendix for Masculinist Actionism: Gender and Strategic Change in US Cyber Strategy," 2024, https://doi.org/10.7910/DVN/XG1RZ0, Harvard Dataverse.
[73]Wajcman, *Feminism Confronts Technology,* 140.
[74]Hutchings, *Masculinity and War*.
[75]In contrast, see: Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (2020): 245–80.

reference gender; it is "just below the surface."[76] Instead, we read the documents to identify the gendered assumptions and logics drawn from the aforementioned literature—namely, military protectionism and tech solutionism—within US cyber strategy.

Second, we contextualize our analysis of the policy documents through an examination of expert commentary on the 2018 US cyber strategic shift, which we source systematically with structured searches from the influential War on the Rocks and Lawfare blogs. The purpose of these sites, which are central to the US cyber policy community, is to literally make sense of the formal policies and their implications. Due to their evaluative function, these commentaries help to connect the implicit structural and conceptual gender dynamics found in the policy documents with more substantive intersubjective gendered assumptions and beliefs. Some commentaries are written by the same people authoring the policy documents; however, this commentary is a more open site of contestation over US cyber strategy. It encourages its participants to speak in plainer language, making the connection between societal gender dynamics and cyber strategy more apparent.

Third, to triangulate our account of the interaction of military and tech masculinities in conditioning US cyber strategic change, we refer to non-systematically sourced, more unusual empirical sites, such as job advertisements, journalistic accounts of workplace dynamics, and biographical details of US cyber operations leaders. These materials demonstrate that the structural gender relationships and implicit conceptual/ideational assumptions seen in the policy documents exist in a daily gendered "normality" of Cyber Command and other military cyber institutions.[77] They connect the gender dynamics we identify in cyber strategy with broader US gender norms, avoiding artificially sealing CYBERCOM and the Department of Defense (DoD) off from society. We use them to substantiate our reading of the structural and conceptual gender hierarchies in policy documents concerning societal and institutional dynamics.[78]

Masculinities and US Cyber Strategic Change

In this section, we empirically make our argument by examining US cyber strategy. First, we demonstrate the role of gendered hierarchy—and the valorization of masculinized action above feminized notions of passivity

[76]Carol Cohn, "Emasculating America's Linguistic Deterrent," in *Rocking the Ship of State: Toward a Feminist Peace Politics*, ed. Adrienne Harris and Ynestra King (Boulder: Westview Press, 1989), 160; Duncanson and Eschle, "Nuclear Weapons State," 552.

[77]Annica Kronsell, "Methods for Studying Silences: Gender Analysis in Institutions of Hegemonic Masculinity," in *Feminist Methodologies for International Relations*, ed. Brooke Ackerley, Maria Stern, and Jacqui True (Cambridge: Cambridge University Press, 2006), 109.

[78]Kronsell, "Sexed Bodies," 316.

and vulnerability—in bounding strategic change through an examination of cyber deterrence up to and throughout the Obama administration. Next, we demonstrate how changes *within* this hierarchy facilitate strategic change through an examination of the 2018 shift toward the concepts of "persistent engagement" and "defending forward", largely during the Trump administration. The interaction of military and tech masculinities produced a change in the contextual meaning of masculinist action, enabling these previously devalued concepts to be constructed as "doing something."

Gendering Cyber Deterrence(s)

Strategists have applied the concept of deterrence to cyber issues since the early 1990s, reflecting evolving strategic concerns coming out of the Cold War.[79] As Fischerkeller, Goldman, and Harknett observe, "the 'deterrence default' [in cyber strategy] was reinforced by a national security enterprise dominated for nearly two generations by deterrence thinking."[80] In inheriting deterrence, US cyber strategy also inherited its construction within the gendered logic of protection previously outlined.

The 2003 National Strategy to Secure Cyberspace, for instance, identifies a need to "deter those with the capabilities and intent to harm our critical infrastructures."[81] It also includes a commitment to "respond in an appropriate manner" to cyberattacks.[82] As such, the document frames cyber deterrence as both a matter of national security and as requiring an active response. The DoD's 2006 National Military Strategy for Cyber Operations likewise draws heavily on deterrence terminology, seeking "military strategic superiority in cyberspace" to "defend cyberspace, critical infrastructure, the homeland, and other vital US interests."[83] The gendered logic of protection animated within conventional deterrence is clear here, as the pursuit of military supremacy (i.e., "strategic superiority") is legitimated and necessitated by its framing as protective of a vulnerable and feminized target ranging from the civilian "homeland" to (US) "cyberspace" itself.[84] Through this logic, these documents construct deterrence in accordance with the values of military masculinity and as a form of martial action. Facilitated by this implicit legacy of masculinized martial legitimacy,

[79]James Der Derian, "Cyber-Deterrence," *Wired*, September 1, 1994, https://www.wired.com/1994/09/cyber-deter/. See also Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996): 93–107.

[80]Michael Fischerkeller, Emily Goldman, and Richard Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022), 5.

[81]The White House, "The National Strategy to Secure Cyberspace," The White House, February 2003, https://www.hsdl.org/?view&did=1040, 6.

[82]White House, "National Strategy," vii; 50.

[83]Peter Pace, "National Military Strategy for Cyberspace Operations," *U.S Department of Defense,* December 2006, http://www.bits.de/NRANEU/others/strategy/07-F-2105doc1.pdf, ix.

[84]Duncanson and Eschle, "Nuclear Weapons State."

deterrence became one of twelve key aims in the 2008 US Comprehensive National Cybersecurity Initiative.[85]

However, the gendering of cyber deterrence is relational, contextual, and subject to change. This gendering is evident within strategic debates that distinguish between deterrence-by-punishment and deterrence-by-denial: preventing attacks by threatening a retaliatory strike that would severely damage or annihilate an adversary, or, conversely, by convincing them that they would not succeed.[86] Early cyber strategic thinking within academia and policy circles discussed deterrence-by-punishment extensively. However, strategists questioned its feasibility in terms of "destructive" cyber-attacks alone, relying instead on cross-domain linkages (i.e., responding to a cyber operation with kinetic force).[87]

Deterrence-by-punishment mirrors the masculinized agency of the gendered logic of protection. As Cohn observes, defense intellectuals construct nuclear deterrence-by-punishment through masculinist norms of objectivity, rationality, and a willingness to kill.[88] Though they legitimate deterrence-by-punishment as a righteous, protective, action, the accumulation (and potential use) of "overwhelming" force renders punishment a form of offense-seeking masculinist control. In US cyber strategy, deterrence-by-punishment introduces a commitment to domination and violence in forms that resemble conventional military offensive potential.[89]

In contemporaneous cybersecurity, however, deterrence-by-denial—hardening networks, air-gapping or segregating systems, limiting user access, patching known vulnerabilities, implementing intrusion detection and prevention, and so on—was as influential, if not more so, than punishment.[90] Early Obama-era cyber strategy "emphasized denial-based approaches such as improving cyber defense and resilience… and sought to limit the application of military power."[91] Although understood in policy terms as deterrence-by-denial, this concept was almost unrecognizable to

[85]The White House, "The Comprehensive National Cybersecurity Archives," *Office of the President*, 2009, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

[86]Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966); Amir Lupovici, "Deterrence through Inflicting Costs: Between Deterrence by Punishment and Deterrence by Denial," *International Studies Review* 25, no. 3 (2023).

[87]Nye, "Nuclear lessons"; Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016): 66–73; Erik Gartzke and Jon R. Lindsay, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019).

[88]Carol Cohn, "Wars, Wimps, and Women," in *Talking Gender and Thinking War*, ed. Miriam G. Cooke and Angela Woollacott (Princeton: Princeton University Press, 1993).

[89]While cyber "Pearl Harbors" are popular in the literature, the development/use of cyber capabilities equivalent to kinetic military operations is regarded with scepticism by most cyber scholars. Cyber capabilities are dependent on a shifting internet architecture, making holding targets "at risk" extremely difficult. Florian Egloff and James Shires, "The Better Angels of our Digital Nature? Offensive Cyber Capabilities and State Violence," *European Journal of International Security* 8 no.1 (2023): 130–49.

[90]Wilner, "Cyber Deterrence," 259.

[91]Lonergan and Schneider, "Power of Beliefs," 2.

practitioners, who largely saw such actions as longstanding, quotidian cybersecurity requirements.

The technical complexity and fluidity of cyberspace, however, means deterrence-by-denial is difficult to construct as solely a national security issue, let alone a military one.[92] Deterrence-by-denial foregrounds cooperation with the private sector and like-minded international counterparts through defensive actions like information sharing, incident response, and systems resiliency. Deterrence-by-denial thus contradicts key commitments of the gendered logic of protection, namely state-centrism, the primacy of the military in national defense, and a masculinized obligation to repel all potential attacks. Deterrence-by-denial's acceptance that cyber incidents happen and the consequent emphasis on building resilient systems rather than offensive cyber capabilities, is antithetical to the conventions of military masculinity, which is necessitated, legitimated, and defined by the protection of feminized dependents.

A 2011 DoD Cyberspace Policy report illustrates the primacy of denial for cyber strategy: only "should the 'deny objectives' element of deterrence not prove adequate, DoD maintains… the ability to respond militarily in cyberspace and in other domains," including "using cyber and/or kinetic capabilities."[93] Here, although the threat of cyber and conventional violence remains, it is preceded by actions practically indistinguishable from defense. This altered emphasis on strategic priority and institutional authority presents a gendered dilemma. At the strategic level, deterrence-by-punishment invokes action, martiality, and protective masculinity—Slayton's cyber "cult of the offensive"—but cybersecurity practice was more reactive, technical, and "defensive."

Subsequent US cyber strategy documents continue to reflect both this martial expectation of masculinized action and attempts to manage it. A policy report presented to Congress in December 2015 highlights several conceptual and practical difficulties in cyber deterrence, including asymmetry between offense and defense, a multiplicity of adversaries, and poor information in terms of attribution and signaling.[94] Though the report mentions deterrence by cost imposition (i.e., punishment), it spends significant time on deterrence-by-denial, emphasizing "defense, resilience, and reconstitution."[95] It implicitly suggests that some kinds of cyber

[92]Such spillover reflects a gendered difficulty in understanding cyberspace itself as a proper object of military action and violence – another avenue for future work.

[93]US Department of Defense, "Department of Defense Cyberpolicy Report," *Department of Defense*, 2011, https://irp.fas.org/eprint/dod-cyber.pdf, 2–4.

[94]These are the same reasons cyber deterrence later fell out of favor amongst key scholars. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93; for an attempt to rescue deterrence, see Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71.

[95]The White House, "Report on Cyber Deterrence Policy," *The White House*, December 2015, https://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf, 6;

operations against the United States are strategically acceptable through the statement that "some networks and infrastructure… are more critical than others."[96] In this document, deterrence-by-denial's emphasis upon "resiliency" and "reconstitution," as well as enduring low-level attacks, suggests an acceptance of vulnerability at odds with masculinized military agency. The contrast of deterrence-by-denial with deterrence-by-punishment, combined with its association with feminized tropes of forbearance and leniency, relationally feminized deterrence-by-denial.

The 2015 DOD Cyber Strategy expresses the same ambivalence. The strategy is ostensibly aimed at "convincing a potential adversary that it will suffer unacceptable costs"—a conventionally martial, masculinized commitment to violent action.[97] However, it gives more space to nonmilitary response options, such as criminal indictments.[98] Consequently, although, as Wilner notes, "Obama's legacy is marked by the rise of cyber offensive measures in US cyber deterrence doctrine," such measures remained subordinate to the administration's general foreign policy emphasis on cooperation and diplomacy.[99] Obama, as observed by Kaminska, sought to "'think differently about our security' and take a public health model in dealing with problems in the cyber domain, which are more akin to viruses and pandemics than 'a bunch of tanks rolling at you.'"[100] The result was an implicit construction of deterrence as "not war," and its conduct, by association, as "not martial masculinity": as inactive.

Obama-era US cyber strategy thus risked contravening the masculinized strategic commonsense of the existing gender hierarchy. Using the term "deterrence" for the defensive, resilience-oriented practices of denial—though likely intended to legitimate those same practices through their associations with national security and martiality—also introduced gendered expectations of masculinist action associated with conventional deterrence. Rather than legitimating deterrence-by-denial through its association with deterrence-by-punishment, the opposite occurs. Obama-era cyber strategy transferred the gendered associations of "deterrence-by-denial," with denigrated, feminized tropes of weakness, vulnerability, and forbearing resilience, to "deterrence" writ large, combining with a lack of credibility in the application of punishment logics to cyber actions to

Sean Lyngaas, "White House Sends Cyber Deterrence Policy to Congress," *FCW*, December 17, 2015, https://fcw.com/articles/2015/12/17/lyngaas-congress-cyber-deterrence.aspx.

[96]White House, "Cyber Deterrence Policy," 6; for example, see: Florian Egloff and Myriam Dunn Cavelty, "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics," *Journal of Cybersecurity* 7, no. 1 (2021): 1–12.

[97]White House, "Cyber Deterrence Policy," 11.

[98]Lonergan and Schneider, "Power of Beliefs," 5.

[99]Wilner, "Cyber Deterrence," 259.

[100]Monica Kaminska, "Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks," *Journal of Cybersecurity* 7, no. 1 (2021): 10.

undermine the authority of cyber deterrence within the national security community.

Obama-era cyber strategy received significant criticism from inside the administration and the broader policy community. Critics saw Obama-era achievements in establishing cyber norms—through the 2013 and 2015 consensus reports of the UN Group of Governmental Experts (GGE) and a 2015 agreement with China restricting "commercially motivated" cyber espionage—as talk shops, or worse, as conceding to adversaries without a fight.[101] Lonergan and Schneider even frame the DoD contribution to these landmarks as "non-action, or deterrence," further underlining the passive construction of deterrence.[102]

In an encapsulation of the masculinized valorization of martial action, Healey observes, "it is not in the nature of professional militaries to passively wait for a blow which is certain to fall."[103] In 2015, the head of the NSA and Cyber Command similarly testified to the House of Representatives that the current "purely reactive defensive strategy is not, ultimately, I think, going to change the dynamic where we are now… I don't think [it] is acceptable to anyone."[104] This lack of authority and legitimacy is attributable to the strategy's inability to meet masculinized expectations of martial agency and offense.

Likewise, in 2015—after the high-profile OPM and Sony Pictures cyber incidents—Senator John McCain condemned the administration's "refusal to articulate a robust strategy to deter cyberattacks," explicitly connecting robustness to punishment ("carry real consequences") rather than the "weak cyber strategy" of denial.[105] McCain's claim follows a gendered logic, although it does not use explicitly gendered language. He accuses the Obama administration of, in essence, accepting a stance of "inaction" through the reliance on "weak" deterrence-by-denial, thus not only contesting a protective, agential martial reading of denial, but also, via association, framing the administration itself as weak and feminized. Later, Obama's own chief cyber policymaker characterized the administration's response to Russian election interference as "frankly inadequate… not apt

[101]Our analysis suggested cyber norms may be relationally feminized. Norm creation takes time, is difficult to assess, and relies on diplomatic relationships. Given the association of norms within global governance frameworks, international law and the State Department, norms were rarely constructed as martial. Consequently, it was difficult to align cyber norms with the masculinist logics of protection and action that conditioned strategic plausibility.

[102]Lonergan and Schneider, "Power of Beliefs," 3.

[103]Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 2.

[104]CSPAN, "Cybersecurity Policy," streamed live on September 29, 2015, 44:37–45:13, https://www.c-span.org/video/?328411-1/hearing-cybersecurity-policy.

[105]John McCain, "Letter to Director of National Intelligence James Clapper," United States Senate, November 18, 2015; Scott Maucione, "McCain Presses Obama Administration on Cyber Deterrence," *Federal News Network*, November 10, 2015, https://federalnewsnetwork.com/defense/2015/11/mccain-presses-obama-administration-cyber-deterrence/.

to be terribly effective, and we knew it."[106] Put more bluntly by another: "I feel like we sort of choked."[107]

As the gendered logic of protection casts an actively masculine military as the protector of a weak, passive, feminized society, then the attachment of attributes of weakness, passivity, and reactivity to deterrence is a discrediting feminization of Obama-era cyber strategy overall.[108] Gender hierarchies act as boundaries for acceptable cyber strategy, and implicitly, for subsequent strategic change.

Institutional Military Masculinity

Our analysis substantiates these contestations regarding the relationship between cyber strategy, deterrence, and martial, masculinized agency at the institutional level. This is most apparent in debates over fitness-for-purpose and status of cyber operators (i.e., the practitioners of deterrence, mostly by denial). Bluntly, cyber personnel struggled to integrate into military structures and institutions, a problem that existed before the Obama administration but became more acute with the creation of US Cyber Command (CYBERCOM) in 2009.

CYBERCOM military leaders referred to the need for personnel to "speak infantry."[109] Conventional military commanders tasked with working with CYBERCOM personnel complained that cyber operators used "unintelligible 'dolphin speak,'" employing technical jargon far removed from typical military concepts.[110] The use of "dolphin" invokes a form of speech associated (not unlike dolphins themselves) with young women, characterized by "squealing" and over-excited, noisy group expressions of enthusiasm.[111] These are tropes associated with the vocal policing of women; more feminine registers are critiqued as "squeaky" and annoying, while women's adoption of lower registers is perceived as artificial.[112] Comparing cyber operators to dolphins, therefore, implicitly denigrates cyber expertise through feminized tropes. It constructs them as, like young women,

[106]Kaminska, "Conditions of Uncertainty," 3.

[107]Ibid.

[108]Bobbi Van Gilder, "Femininity as Perceived Threat to Military Effectiveness: How Military Service Members Reinforce Hegemonic Masculinity in Talk," *Western Journal of Communication* 83, no. 2 (2019): 151–71.

[109]Sydney Freedberg, Jr., "Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'," *Breaking Defense*, November 10, 2015, https://breakingdefense.sites.breakingmedia.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

[110]Freedberg, "Culture Gap."

[111]For example, see: Maureen O'Connor, "Why Adult Women Squeal Like Teen Girls Sometimes," *The Cut*, December 10, 2013, https://www.thecut.com/2013/12/why-adult-women-squeal-like-teen-girls-sometimes.html; Monika Chao and Julia Bursten, "Girl Talk: Understanding Negative Reactions to Female Vocal Fry," *Hypatia* 36 no. 1 (2021): 42–59.

[112]Milena Droumeva, "From Sirens to Cyborgs: The Media Politics of the Female Voice in Games and Game Cultures," in *Feminism in Play*, ed. Kishonna Gray, Gerald Voorhees, and Emma Vossen (Palgrave Macmillan, 2018), 51–67.

appearing in spaces they do not belong and claiming authority to which they are not "entitled."[113]

Similarly, as cyber operations became more integrated into conventional national and military security, military commentators strongly contested initiatives to recognize their efforts. For instance, military personnel resisted plans to elevate a proposed Distinguished Warfare Medal recognizing exceptional service that need not involve combat above the Purple Heart, which is awarded by the US military in the name of the president for physical bravery.[114] One commentator argued:

> [T]o rank what is basically an award for meritorious service higher than any award for heroism is degrading and insulting to every American Combat Soldier, Airman, Sailor or Marine who risks his or her life and endures the daily rigors of combat in a hostile environment.[115]

The heroism accrued through the performance of stereotypical military masculinity, involving bravery, risk, and proximity to violence, trumps technical cyber expertise.[116]

Even within cyber expert ranks, gendered hierarchies favored more combat-oriented roles. As Slayton argues, investigating intra-service dynamics well before the Obama administration:

> Threat-focused activities like offensive operations, intrusion detection, and incident response… were most easily viewed as warfighting. By contrast, vulnerability-focused activities such as password management, software patching, and other forms of technology maintenance… were slow to be seen as a kind of warfighting.[117]

"Warfighting," and its connotation of masculinized military agency, is the arbiter of authority and priority for cyber operators. Militarized masculinity both distinguishes cyber operators from "real" soldiers and hierarchizes them amongst themselves, tracking their proximity to masculinized "combat."[118]

Across the Obama administration, as phrased by Freedberg, a sense arose that cyber operations were "too important to leave to the cyber geeks," creating incentives for cyber operators to try to become less geeky, more military, and more warfighting.[119] These hierarchies led to explicit comparisons with long-mythologized and sought-after military branches. One RAND study argued that, like Special Operations Forces, "cyber forces need and value an entirely different set of skills [to combat forces],

[113]Anne Carson, "The Gender of Sound: Description, Definition and Mistrust of the Female Voice in Western Culture," *Resources for Feminist Research* 23, no. 3 (1994): 24.
[114]Lin, "Doctrinal Confusion," 97.
[115]Military Order of the Purple Heart, as cited in Lin, "Doctrinal Confusion," 97.
[116]The DWM was subsequently cancelled.
[117]Slayton, "Cyber Warriors," 63.
[118]Barrett, "Hegemonic Masculinity."
[119]Freedberg, "Culture Gap."

including unique technical skills and other 'geek arts.'"[120] The development of "concepts of cyber operations that were analogous to well-established concepts of kinetic operations" also reflected intra-cyber hierarchies.[121] It mirrors, at the operational level, the way invocations of "deterrence" at the strategic level sought legitimation through association with military masculinity.

The move to reframe cyber operators as "cyber warriors" illustrates two parallel strategic dynamics. First, it shows how agential, protective military masculinity bounds strategic commonsense. The attempt to valorize (some) technical cybersecurity skills resists their total conflation with deterrence-by-denial and concomitant associations of weakness and passivity. Second, however, this move subtly points toward the potential for cyber strategic discourse to construct technical cybersecurity concepts and skills not as martial but, drawing upon alternative logics of gender, as similarly masculine. In the next section, we outline how references to flexibility, technical skill, and problem-solving—characteristics of idealized tech masculinity—facilitated the 2018 strategic shift from deterrence to "persistent engagement" and "defending forward" through a change in what counts as masculinized action.

Persistent Engagement, Defend Forward, and Gendered Strategic Change

In 2018, US cyber strategy underwent substantial revision, adopting the new strategic concepts of "defending forward"—cyber operations intended to counter adversaries outside "home" networks, in allied or adversary spaces—and "persistent engagement": constant low-level, tactical or operational contact between adversaries, seeking to detect and remove the adversary's footholds in one's networks while simultaneously looking to stealthily hack into theirs, all without triggering escalation.

The 2018 Cyber Command Strategic Vision framed defending forward as part of a broader goal of "persistently contest[ing] malicious cyberspace actors."[122] Similarly, the 2018 DoD Cyber Strategy identifies defending forward as one means to persistently contest adversaries (a view also articulated by the head of Cyber Command).[123] In contrast, the 2018 National Cyber Strategy used "persistent engagement" to describe cyberspace interactions without mentioning defending forward.[124] Although

[120]Christopher Paul, Isaac Porche, III, and Eliot Axelband, "The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces" (Santa Monica: RAND Corporation, 2014), 40.
[121]Slayton, "Cyber Warriors," 63.
[122]US Cyber Command, "Achieve and Maintain Cyberspace Superiority," *US Cyber Command*, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.
[123]Paul Nakasone, "An Interview with Paul M. Nakasone," *Joint Forces Quarterly*, no. 92 (2019): 10–14. For Nakasone, one third of persistent engagement is acting, and "acting includes defending forward": Nakasone, "Interview," 7.
[124]White House, "National Cyber Strategy 2018."

analysts of persistent engagement and defending forward have highlighted their lack of clarity and ambiguity, most now agree that persistent engagement is the broader concept, describing a wide range of cyber operations under the threshold of armed conflict while defending forward is a specific tactic within persistent engagement referring to activities in allied or partner states. Practically, although defending forward involves similar practices to deterrence-by-denial at the tactical level, it differs significantly in where these practices take place and their strategic interpretation.

The constant activity involved in persistent engagement is a significant strategic shift from the need for highly impactful capabilities to be held "in reserve" for deterrence-by-punishment. To facilitate this change, Trump elevated Cyber Command to a Unified Combatant Command in August 2017, with a subsequent full operationalization of its cyber mission forces. In 2018, Trump also issued a Presidential Finding and Executive Order reducing the legal and bureaucratic constraints on offensive cyber operations for the CIA and Cyber Command. The DoD likewise updated its cyber operations manual in 2018, while lawmakers incorporated new attempts to reduce interagency friction into the 2019 National Defense Authorization Act.

Gendered portrayals of this shift abound in the Trump administration's discourse on cyber strategy. According to Trump's National Security Advisor, these changes had a single purpose: "we need to start competing more aggressively with our adversaries in cyberspace."[125] Vice-President Pence claimed the Obama administration had "chose[n] silence and paralysis over strength and action"—a condemnation based on the sexist and ableist denigration of purported dependence, weakness, and passivity—before proclaiming in classic martial fashion: "gone are the days that America allows our adversaries to cyberattack us with impunity."[126] As articulated by a senior cyber official, the Trump National Security Council began from a position of "stop the bleeding, stop building things that bleed, and make the other guy bleed."[127] This portrays cyber operations as an aggressive clash of combat violence—and avoiding the feminized act of shedding blood.[128] Such visceral language was echoed by others, as one influential former NSA cybersecurity expert described the US strategic shift as "trying to figure out how to kick them [US adversaries] in the

[125]Garrett Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army," *Wired*, October 13, 2020, https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/.

[126]Mike Pence, "Remarks by the Vice President at the Department of Homeland Security Cybersecurity Summit in New York City," *The American Presidency Project*, July 31, 2018, https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-department-homeland-security-cybersecurity-summit-new-york.

[127]Graff, "Big Cyber Army."

[128]See: Holly Yan, "Donald Trump's 'Blood' Comment about Megyn Kelly Draws Outrage," *CNN*, August 8, 2015, https://edition.cnn.com/2015/08/08/politics/donald-trump-cnn-megyn-kelly-comment/index.html.

balls."[129] The administration demonstrated a concern with redeeming the masculinity, autonomy, and agency that was ostensibly undermined by Obama-era foreign policy generally and cyber strategy specifically.

Cyber policy experts saw this more "aggressive competition" as a direct response to the perceived failures of deterrence. An influential article by key US academics was titled "Deterrence is Not a Credible Strategy for Cyberspace," framing persistent engagement as its logical successor.[130] A former General Counsel to Cyber Command stressed that: "Neither defend forward nor persistent engagement is intended to be a mode of deterrence. At best, they might serve deterrence ends but only secondarily."[131] Others summarize the Cyber Command Strategic Vision as a "strident rejection of cyber deterrence."[132] According to them, it functions as "a counterargument against the deterrence-based and norms-based strategies of the Obama administration."[133] Both administration officials and expert commentary tied the introduction of persistent engagement and defend forward to the perceived failures of deterrence, with its feminized connotations of passivity and vulnerability. Consequently, the boundaries of acceptability for persistent engagement are set by the inverse attributes: a credible claim to masculinized authority, legitimacy, and action.

Martiality, however, is not the sole source of valorized masculinity for cyber strategy. As outlined earlier, tech masculinity, invoking technical mastery, autonomy, and problem-solving, has grown in prominence within US society and national security communities, introducing an alternative understanding of masculinity, and action, to cyber strategy. During debates over cyber deterrence, the expert diagnosis of deterrence as "ineffective" drew on traces of engineering solutionism by arguing for cyber as a distinct, "complex" security domain, accompanied by an attempt to valorize technical cyber expertise as distinct from, and superior to, conventional military skill.

By the 2018 strategic shift, the values and commitments of tech masculinity start to move from supporting criticisms of deterrence to offering the contours of a legitimately agential, authoritatively masculine alternative. The core appeal of persistent engagement/defend forward is that they are *active*. Harknett summarizes the new US strategy as a "shift away from a reactive posture… proactively seek[ing] to regain its balance and eventually

[129]Kenneth Geers in Alex Lockie, "The US Can Retaliate against Russian Hacking and 'Kick Them in the Balls,'" *Business Insider*, July 21, 2017, https://www.businessinsider.com/us-retaliate-russia-hacking-election-2017-7.
[130]Fischerkeller and Harknett, "Credible Strategy"; Fischerkeller et al., *Cyber Persistence Theory,* 128.
[131]Gary Corn, "SolarWinds Is Bad, but Retreat from Defend Forward Would Be Worse," *Lawfare*, January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[132]Lonergan and Schneider, "Power of Beliefs," 5.
[133]Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

its initiative."[134] Kollars and Schneider interpret the 2018 DoD strategy [as] "much more active and risk-acceptant… view[ing] the main risk to US objectives not as the use of cyber operations but, rather, inaction."[135] The joint head of Cyber Command and NSA Director, Paul Nakasone, is equally clear: the priority is to "operate continuously to seize and maintain the initiative," because "this is a domain that requires constant action… it's the *use* of cyber capabilities that is strategically consequential [emphasis in original]."[136] The Executive Director of Cyber Command puts it succinctly: "success is determined on how we enable and act."[137]

The role of tech masculinity in constituting persistent engagement as active (and therefore acceptable) is most apparent in the strategy's emphasis upon operators acting "seamlessly." Persistent engagement holds that "the analytical categories of offense and defense do not actually hold in this space—it is too fluid and dynamic."[138] It contests the conflation of agency with offense found within the logic of military masculinity. Persistent engagement posits defense as a form of valued agency and challenges the distinction itself as irrelevant. The focus of persistent engagement, furthermore, in contrast to the valorization of combat, is deliberately "under-the-threshold," seeking low-level, (ostensibly) preventative, sometimes even unnoticed interventions. Cyber strategic discourse no longer solely expresses a gendered expectation of action through the righteous use of violence, but also through risk-taking, flexibility/continuity, and initiative, which are traits valorized within tech masculinity.

Despite these differences, idealized tech masculinity shares with conventional military masculinity a gendered aversion to "violation," vulnerability, and feminizing defeat. As Healey notes, the 2018 National Cyber Strategy "emphasized malicious and implacable adversaries rather than American vulnerability."[139] In stark language, one Senator claimed "we're a cheap date when it comes to cyber… people can go after us… and not really expect much in the way of a response."[140] Here, sexist attitudes associated with, at best, a transactional view of heterosexual dating culture or, at worst, the normalization of sexual assault, was used to denigrate

[134]Richard J. Harknett, "SolarWinds: The Need for Persistent Engagement," *Lawfare,* December 23, 2020, https://www.lawfareblog.com/solarwinds-need-persistent-engagement.

[135]Nina Kollars and Jacquelyn Schneider, "Defending Forward: The 2018 Cyber Strategy Is Here," *War on the Rocks,* September 20, 2018, https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.

[136]Nakasone, "Interview with Nakasone."

[137]Todd Lopez, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," *Defense.gov News,* May 14, 2019, https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.

[138]Richard J. Harknett, "Preliminary Written Responses, Cybersecurity Sub-Committee, United States Senate Armed Services Committee," *United States Armed Services, Senate Committee*, February 13, 2018, https://www.armed-services.senate.gov/imo/media/doc/Harknett_02-13-18.pdf, 2.

[139]Jason Healey, "Twenty-Five Years of White House Cyber Policies," *Lawfare*, June 2, 2023, https://www.lawfareblog.com/twenty-five-years-white-house-cyber-policies.

[140]Sydney Freedberg, Jr., "A 'Solarium' for Hacking: Sen. King Launches Cyber Strategy Panel," *Breaking Defense*, May 13, 2019, https://breakingdefense.sites.breakingmedia.com/2019/05/a-solarium-for-hacking-sen-king-launches-cyber-strategy-panel/. Thanks to Monica Kaminska for this reference.

the United States' cyber strategy as feminized and helpless.[141] For this Senator, persistent engagement implied that the United States will not "just sit back and take it."[142]

Unsurprisingly, then, even as tech masculinity shifted the boundaries of acceptability for persistent engagement, advocates continued to deploy tropes of military masculinity to help communicate its commitment to action. An influential article by Nakasone explained persistent engagement as meaning that "we must take this fight to the enemy."[143] Commentators compared the new US strategy to Muhammad Ali's boxing tactics, a classic (if not uncontested) trope of US masculinity, bravery, and physical prowess, as well as agility (the authors' main point).[144] US media portrayed persistent engagement as the cyber equivalent of hand-to-hand combat.[145] The strategy was thus a strikingly active contrast to both deterrence and the purported inefficacy of other contemporaneous efforts, such as a collapse of cybersecurity diplomacy at the 2017 UN GGE.

Defending forward and persistent engagement emerged within and contributed to an environment split between a desire to entirely disavow the feminized failures of deterrence and a belief that deterrence itself could be remade (and remasculinized) to work in combination with these new concepts. The rise of persistent engagement was not due to a total displacement of military masculinity by tech masculinity. Instead, tech masculinity's emergence as an alternative source of masculinized authority and legitimacy redrew the boundaries of acceptable cyber strategy. Masculinist action expanded to include non-offensive, non-combat cybersecurity concepts and practices, rendering persistent engagement acceptable within an overall gendered hierarchy of protective masculinity over vulnerable femininity. The meaning of martial, masculine action was modified by alternative, tech-informed conceptions of masculine authority, action, and security to legitimate the process of strategic change while maintaining the existing gender hierarchy.

This dynamic helps explain the persistence of deterrence within US cyber strategy as a live, if no longer hegemonic, concept. The 2018 DoD Cyber Strategy, for instance, situates persistent engagement within an

[141]This rhetoric reflects a trend within cybersecurity, wherein metaphors associated with heterosexual sex and/or sexual assault – such as "penetration testing" networks for vulnerabilities – are a typical part of the lexicon.

[142]Freedberg, Jr., "'Solarium' for Hacking."

[143]Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, no. 92 (2019): 10–14.

[144]Herbert Lin and Max Smeets, "What Is Absent from the U.S. Cyber Command 'Vision'," *Lawfare*, May 3, 2018, https://www.lawfareblog.com/what-absent-us-cyber-command-vision.

[145]Ellen Nakashima, "New Details Emerge about 2014 Russian Hack of the State Department: It Was 'Hand to Hand Combat'," *Washington Post*, April 3, 2017, https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html. Although this story refers to an earlier incident, it was written in the context of policy debates around persistent engagement.

overall US national security commitment to deterrence.[146] It also employs logics of deterrence—especially by punishment—throughout.[147] As Lonergan and Schneider note, "deterrence sits alongside if not underneath new strategic concepts [of] defend forward/persistent engagement."[148] Within the Trump administration, an unclassified summary of a State Department "assessment of deterring malicious cyber activities" released in May 2018 concurred, concluding deterrence should stay, but "require[s] a fundamental rethinking."[149] Two years later, the 2020 Solarium Commission squared this circle by inventing the concept of "layered cyber deterrence" as an overall framework encompassing persistent engagement.[150]

The interaction of military and tech masculinities also helps explain the trajectory of another candidate strategic concept: active defense. Active defense was developed in the 1990s and rose to prominence in US cyber policy circles in 2012–13 following a series of high-profile Iranian cyber-attacks against the US.[151] To simplify a contested debate, in the United States "active defense" refers to a policy wherein many organizations—from the military to government departments to private companies—would be encouraged to act outside their "home" networks, domestic or worldwide. More specific conceptualizations of "active defense" range from the cyber-security industry concept of "threat hunting" (i.e., internal measures that go beyond "standard" cybersecurity network monitoring to identify and counter malicious actors) to the de facto deputization of non-state actors to "hack back" against cyberattacks.[152]

Active defense epitomizes the values, norms, and priorities associated with tech masculinity: the valorization of cybersecurity skills as authoritative expertise, an emphasis on individuated genius expressed in technical "battle," and a willingness to bend norms of statist protection through the exercise of neoliberal, corporatized, agency. Pushed to an illustrative extreme, "active defense" offers a strategy enacted by a series of decentralized, technologically skilled hackers located in the private sector battling cyberattacks through problem-solving prowess. This is what a strategic concept constituted *solely* in line with tech masculinity might look like.

[146]Department of Defense, "Cyber Strategy 2018," 4.
[147]Wilner, "Cyber Deterrence," 257.
[148]Lonergan and Schneider, "Power of Beliefs," 4.
[149]Office of the Coordinator for Cyber Issues, "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," May 31, 2018, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.
[150]US Cyberspace Solarium Commission, "Final Report," *US Cyberspace Solarium Commission*, March 2020, https://www.solarium.gov/report.
[151]James Shires, *The Politics of Cybersecurity in the Middle East* (Oxford: Oxford University Press, 2022.), 91.
[152]Wilner, "Cyber Deterrence," 268.

Active defense enjoyed one of its recurrent rises in prominence in US cyber policy at a similar time to the embrace of persistent engagement.[153] However, this reliance on tech masculinity helps explain why it has continued to hover on the wrong side of acceptable cyber strategy. Active defense is more difficult to fuse with a martial logic of gendered protection because it undermines the power of the state, in general, and defense and national security, in particular. The discarding of active defense demonstrates that while strategic change is facilitated by shifts in specific contextual gender norms, those norm shifts only go so far. In boundary-setting, gender shapes acceptable cyber strategy by closing out alternatives as well as informing "successful" strategic concepts.

Institutional Tech Masculinity

As with deterrence, our analysis also substantiates the re-negotiation of tech and military masculinities. These at the individual and institutional levels, via a further reevaluation of the soldier-geek relationship. It is now common for commentators to entertain accommodating typically "tech" individuals (usually framed as men) by altering military structures. Suggestions range from creating an "elite corps of genius hackers," "super-empowered individuals," or "brilliant dudes," to "Cyber Direct Commissioning."[154] As in the previous section, commentators still portray such individuals as "hardcore cyber people" or "techies and geeks."[155] They have a minimal amount of interest in military discipline, traditions, and fitness.[156] However, they more openly acknowledge such individuals' value. One commentator suggested that cyber operators are "categorically different than other servicemembers," advising that it might be best to hire cyber operators as civilians, "eliminat[ing] the lost man-hours from required trips to the rifle range."[157] The gendered gatekeeping observed earlier is reversed: the "geniuses" of Cyber Command should be insulated from the strictures of typical military service.

Consequently, commentators began to criticize military masculine hierarchies as harmful to recruitment. A declaration by the Air Force Cyber Commander that he was "not a technologist… [but] a fighter pilot" was reported with the qualifier that "military hackers hear such self-deprecating

[153]Active Defense Cyber Certainty Act, H.R.4036, 116th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/4036.

[154]For the first three quotes, see Sydney J. Freedberg, Jr., "Do Young Humans + Artificial Intelligence = Cybersecurity?," *Breaking Defense*, November 13, 2017, https://breakingdefense.sites.breakingmedia.com/2017/11/do-young-humans-artificial-intelligence-cybersecurity/. For the last quote, see: John Scott Lewinski, "Inside the U.S. Army's New Cyber Command Center," *InsideHook*, April 30, 2018, https://www.insidehook.com/article/military/inside-u-s-armys-new-cyber-command-center.

[155]Graff, "Big Cyber Army."

[156]Lewinski, "Cyber Command Center."

[157]Butch Bracknell, "Who Says Cyber Warriors Need to Wear a Uniform?," *Modern War Institute*, March 23, 2018, https://mwi.usma.edu/says-cyber-warriors-need-wear-uniform/.

qualifications all too often, and it's never received well."[158] Cyber Command's anti-ISIS forceremembered fondly that "we didn't care about rank or service… you were all equals in this fight."[159] The same influences conventional military authorities previously saw as "feminizing" the armed forces also reflected of an alternative model of masculinity gaining prominence within Cyber Command and the DoD, emphasizing technical competence, agility, and speed.

Commentators expressed the influence of tech masculinity in shorthand, comparing stereotypical masculine dress: jeans, T-shirts, and flip flops against suits and ties or combat fatigues. However, tech masculinity is most obvious in hackers' reported motivations for joining the military, including "fast-paced, hectic" work and "the thrill of the challenge [or] the delight of solving a puzzle."[160] One military author notes in wonder that hackers "toil for countless hours looking for vulnerabilities… simply for peer recognition."[161] An oft-cited motivator is an amorphous concept of "mission," rooted in public service, but also the permission and ability to do "cool" things that would otherwise be illegal.[162] An NSA recruitment banner advertised this as "push[ing] the limits of innovation."[163] As a member of Cyber Command's anti-ISIS task force described, "When you reach through the computer and on the other side is a terrorist organization… that is an incredible rush… you have the *control* [emphasis added] to take that away."[164]

The individualism of "genius" hackers is implicitly contrasted with the conformity expected of typical military personnel, shifting the latter from a form of masculine discipline to a more feminized trait of obedience. Earlier cyber operators sought to legitimize their practice mainly through martial connotations; however, the later generations construct very similar technical operations as desirable through their association with ideas of technological control, risk-taking, and boundary-breaking valorized within tech masculinity.

Overall, tech masculinity has emerged alongside military masculinity as an alternative source of institutional authority and legitimacy. This produced a change in the contextual meaning of a specific gender

[158]Josh Lospinoso, "Fish out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It," *War on the Rocks*, July 12, 2018, https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/.

[159]Graff, "Big Cyber Army."

[160]For the first direct quote, see Mike Cerre, "An Exclusive Look behind the Scenes of the U.S. Military's Cyber Defense," *PBS NewsHour*, March 30, 2018, https://www.pbs.org/newshour/show/an-exclusive-look-behind-the-scenes-of-the-u-s-militarys-cyber-defense. For the second, see Freedberg, Jr., "Young Humans + Artificial Intelligence."

[161]Lewinski, "Cyber Command Center."

[162]Cerre, "Behind the Scenes."

[163]Darren Samuelsohn, "Inside the NSA's Hunt for Hackers," *Politico*, September 12, 2015, https://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330/.

[164]Dina Temple-Raston, "How the U.S. Hacked ISIS," *NPR*, September 26, 2019, https://perma.cc/337Y-4ERC.

norm—masculinist action—that enables engineering solutionism to be commensurate with gendered protection. Though existing gender hierarchies are maintained, strategic change within these bounds is facilitated by a gendered shift in what it means to be active.

Conclusion

This article has argued that shifts in specific contextual gender norms—namely, masculinized action—alter the boundaries of acceptable strategic change. We demonstrate this argument by examining the interaction of two modes of masculinity—military and tech—in setting the parameters for US cyber strategic change. After cyber deterrence fell afoul of the masculinized expectations of military masculinity, the ascendance of tech masculinity as an alternative source of gendered authority presented persistent engagement as a viable strategic concept. The interaction of tech and military masculinities maintained the gendered hierarchical, gendered expectation of protective action—"masculinist actionism"—while facilitating strategic change through a shift in the meaning of what counts as action. This shift within modes of masculinity helps to structure and maintain broader gendered hierarchies of masculinity/ies over femininity/ies and action over passivity.

Masculinist actionism is not limited to cyber strategy. The gendered concepts, structures, and intersubjective beliefs that comprise military and tech masculinities extend into contemporary US (and Western) society beyond the national security institutions considered here and share the qualities of autonomy, rationality, and agency that also characterize broader, non-national security masculinities. Therefore, our argument suggests that contemporary strategic change is conditioned by the ability to construct new concepts as not only agential, but agential in a particular way: simultaneously the righteous violence of military masculinity *and* the rapid, "agile" response of technical problem-solving. The gendered constitution of strategic change via masculinist actionism is analytically generalizable.

Understanding strategic change thus requires a careful analysis of the role of gender in shaping not only the identity of institutional actors but also the gendered structures, relations, and intersubjective values, beliefs, and assumptions that constitute what they do, the environment in which they act, and bounds of what can be considered "logical." This has two implications for policy. First, policymakers in cyber strategy and beyond would be well-advised to consider not only institutional culture, strategic environment, and bureaucratic incentives but also how gendered constructions of authority, priority, and legitimacy condition the meaning of

strategic concepts. Strategic revisionism requires engaging with gender structures and expectations as a dimension of power.

Second, our analysis adds further credence to feminist accounts that caution against assuming the greater participation of women, people of diverse gender identities, expressions, and sexualities, and minoritized people within strategic policymaking and governance—though vital from the perspective of equality—will lead to the automatic incorporation of new and alternatively ethical perspectives into strategy. Not only do such presumptions risk essentialism, they fail to account for the importance of institutional gender norms, assumptions, and expectations: all of which may be experienced by all people, regardless of embodied gender identification and expression.

Acknowledgments

The authors would like to thank Yuna Han, Monica Kaminska, Gustav Meibauer, Woohyeok Seo, Max Smeets, Peter Trubowitz, the *Security Studies* editorial team, and particularly the journal's three anonymous reviewers for their insightful comments and productive engagement with this article.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Appendix

Table A1. Policy documents.

Document	Date	Actor
Presidential Policy Directive PPD63	1998	WH
National Strategy to Secure Cyberspace	2003	WH
National Military Strategy for Cyber Operations NMS-CO	2006	DOD
Comprehensive National Cybersecurity Initiative	2008	WH
Keith Alexander nomination questions	2010	Congress
Keith Alexander testimony to Armed Services Sub-Committee	2010	Congress
Cyber Command factsheet	2010	DOD
Strategy for Operating in Cyberspace	2011	DOD
NDAA Cyberspace Policy Report	2011	DOD
International Strategy for Cyberspace	2012	WH
Presidential Policy Directive PPD20	2012	WH
Defense Service Board Advanced Cyber Threat	2013	DOD
Keith Alexander testimony to Armed Services Committee	2013	Senate
Mike Rogers testimony to Select Intelligence Committee	2014	Congress
Intelligence heads testimony to Select Intelligence Committee	2015	Congress
Intelligence heads testimony to Select Intelligence Committee v2	2015	Congress
Cyber Strategy	2015	DOD
Defense Service Board Task Force Cyber Deterrence	2017	DOD
Rogers/Clapper/Lettre testimony to Armed Services Committee	2017	Senate
Mike Rogers testimony to Armed Services Committee	2017	Senate
Intelligence heads testimony to Armed Services Committee	2017	Senate
Executive Order on Strengthening cybersecurity	2017	WH
National Security Strategy	2017	WH
Mike Rogers statement to Armed Services Committee	2018	Senate
National Defense Strategy (unclassified summary)	2018	DOD
Cyber Command Strategic Vision	2018	DOD
Joint Chiefs of Staff Publication 3(12) Cyberspace Operations	2018	DOD
Cyber Strategy (summary)	2018	DOD
National Cyber Strategy	2018	WH
National Defense Authorization Act for 2019	2018	Senate
National Defense Authorization Act for 2019 Amendment	2018	Senate
National Defense Authorization Act for 2019	2019	Congress
National Security Presidential Memorandum 13	2018	WH
Paul Nakasone confirmation hearing Armed Services Committee	2018	Senate
Richard Harknett testimony to SASC	2018	Senate
Michael Sulmeyer testimony to SASC	2018	Senate
Presidential finding authorizing CIA cyber operations	2018	WH
Paul Nakasone statement to Armed Services Committee	2019	Senate
Paul Nakasone interview in Joint Forces Quarterly	2019	JFQ
Solarium Commission Final Report	2020	Senate/Congress
Paul Nakasone Statement to Armed Services Committee	2020	Congress
Paul Nakasone Statement to Armed Services Committee	2021	Senate
Interim National Security Strategic Guidance	2021	WH
Paul Nakasone testimony to Armed Services Committee	2021	Congress

Table A2. Expert commentary.

Author	Venue	Date
Lin	Lawfare	2016
Snyder and Sulmeyer	Lawfare	30/1/2017
Sulmeyer	WOTR	19/7/2017
Sulmeyer	WOTR	31/8/2017
Sulmeyer	Lawfare	19/12/2017
Sulmeyer	Foreign Affairs	22/3/2018
Harknett	Lawfare	23/3/2018
Lin and Smeets	Lawfare	3/5/2018
Lospinoso	WOTR	12/7/2018
Chesney	Lawfare	26/7/2018
Flournoy and Sulmeyer	Foreign Affairs	14/8/2018
Weinstein	Lawfare	21/9/2018
Buchanan	CFR	25/9/2018
Chesney	Lawfare	25/9/2018
Fischerkeller and Harknett	Lawfare	9/11/2018
Valeriano and Jensen	CATO	15/1/2019
Fischerkeller and Harknett	Lawfare	19/2/2019
Smeets	Lawfare	20/3/2019
Schoka	WOTR	3/4/2019
Fischerkeller and Harknett	Lawfare	15/4/2019
Miller and Pollard	Lawfare	30/4/2019
Schneider	Lawfare	10/5/2019
Lopez	Defense.gov	14/5/2019
Jensen	WOTR	20/6/2019
Fischerkeller and Harknett	Lawfare	27/6/2019
Myre	NPR	26/8/2019
Rovner	WOTR	16/9/2019
Campbell	Lawfare	18/9/2019
Fischerkeller and Harknett	Lawfare	6/2/2020
Smeets and Soesanto	CFR	18/2/2020
Maschmeyer	Lawfare	4/3/2020
Jensen	Lawfare	11/3/2020
Borghard and Montgomery	Lawfare	11/3/2020
Bate et al.	Lawfare	11/3/2020
Borghard	Lawfare	12/3/2020
Rovner	WOTR	19/3/2020
Harknett	Lawfare	23/3/2020
Fischerkeller	Lawfare	23/3/2020
Borgharad	CFR	22/4/2020
Fischerkeller	WOTR	24/6/2020
Nakasone and Sulmeyer	Foreign Affairs	25/8/2020
Anderson, Fleischaker, and Russell	WOTR	7/9/2020
Jasper	CFR	13/7/2020
Rovner	WOTR	14/9/2020
Shires, Chesney, and Smeets (eds.)	TNSR	17/9/2020
Graff	Wired	13/10/2020
Greenberg	Wired	14/10/2020
Borghard and Schneider	Wired	17/12/2020
Valeriano, Jensen, and Montgomery	Lawfare	18/12/2020
Morgus	Lawfare	18/12/2020
Valeriano	CFR	21/12/2020
Fischerkeller and Harknett	Lawfare	23/12/2020
Corn	Lawfare	14/1/2021
Poznansky	WOTR	23/3/2021
Kaminska	CFR	31/3/2021
Newman	Wired	06/04/2021
Fischerkeller	Lawfare	22/4/2021
Sherman and Herr	CFR	26/4/2021

Table A3. Media reporting.

Author	Venue	Date
Conti and Easterly	Small Wars Journal	29/7/2010
Reed	Foreign Policy	24/10/2012
Tilghman	Military Times	4/8/2014
Freedberg	Breaking Defense	10/11/2015
Pomerleau	C4ISRnet	12/10/2017
Freedberg	Breaking Defense	13/11/2017
Bracknell	Modern War Institute	23/3/2018
Gerre	PBS	30/3/2018
Lewinski	Inside Hook	30/4/2018
Pomerleau	Fifth Domain	3/8/2018
Temple-Raston	NPR	26/9/2019
Pomerleau	Fifth Domain	12/2/2020
Maucione	Federal News Network	26/10/2020
Press release	Cyber Command	6/7/2021