Masculinity can influence cyber strategy

James Shires *and* **Kate Millar** *examine how different kinds of masculinity shape the evolution and implementation of modern cyber defence strategies in the United States and beyond.*

In 2023, the US Cyber Command deployed specialist cybersecurity teams 22 times to help find vulnerabilities in the networks of partner countries. This marked a significant expansion from around 50 deployments across the previous five years. The programme, known as “Hunt Forward”, has gathered much momentum among cybersecurity policymakers but is highly controversial. Supporters point to how it practically contributes to the partner state’s cyber defences and helpfully adds new data to public cybersecurity repositories. However, critics point to undeclared intelligence collection opportunities and the escalation risks from adversaries’ perception of direct US involvement.

The United States is not alone in conducting hunt-forward operations. The United Kingdom has also stated that it conducts such operations, and Canada has collaborated with the US on hunt-forward campaigns. A recent review of such operations was published by the UK defence company BAE Systems, which has a significant stake in international cybersecurity capacity-building, including in places like Ukraine where hunt-forward operations have been deployed.

The review emphasised that they are “purely defensive operations, but the label of ‘hunt forward’ can lead to them being misunderstood as offensive”. At the London conference where this report was launched in November 2023, several attendees lamented the name ‘hunt forward’, saying that although it created confusion, it was necessary to sell cyber defence operations internally within the military hierarchy.

What’s in a name?

In a recent article, Kate Millar and I put forward a perhaps surprising suggestion: that

gender creates informal requirements for what constitutes a good operation or strategy. We refer to this phenomenon as “masculinist actionism”. Drawing upon the work of Brent Steele, we argue that militaries and other state institutions are caught in the midst of a broader social change between two idealised forms of masculinity. The first is “martial masculinity,” which valorises the traditional warrior willing to fight and die for his country. The second is “tech masculinity,” which celebrates the stereotypical geek who finds ways to unravel technologies through individual genius – and social awkwardness. In short, Rambo and Mr Robot, James Bond and Q.

This interaction between masculinities plays out across society, in films, media, and individual career decisions. It manifests in state institutions such as the military through stereotypical masculine dress: jeans, T-shirts, trainers and flip-flops for tech masculinity (not to mention the cliched hacker hoodie) as opposed to suits and ties or combat fatigues for military masculinity.

There are also more pernicious and problematic manifestations. Journalist Barton Gellman’s summary of US National Security Agency (NSA) code names for different stages of a cyber operation, discovered as part of the Edward Snowden leaks, included titles like BLINDDATE, HAPPYHOUR, NIGHTSTAND, and SECONDDATE, culminating in PANT_SPARTY. He concluded that “sexual exploitation is an official metaphor of [cyber] operations, passed up the chain of command in operations reports and back down to the lower ranks in training materials”.

Gendered policies

Gendered distinctions also emerge in policy throughout the history of cyber operations. US Army officer and academic researcher Sarah P. White traces the history of US Navy cyber operators back to pre-1995 restrictions on women in combat and the consequent formation of the shore-based General Unrestricted Line Community (GURL), which specialised in electronic communications. The naming of this group is surely not coincidental, with gendered – and indirectly demeaning – designations devaluing the status of cyber operations (at least then).

The gendering of cyber strategy means that policymakers must satisfy not only a whole host of political and bureaucratic constraints in introducing strategic change but also manoeuvre within boundaries set by the influences of this dual masculinity.

What does this look like in practice? ‘Hunt forward’ offers some clues. A label that practitioners find cumbersome and diplomats awkward nonetheless became the key framing for the strategy. Why? Because alternatives, like BAE’s distinctly unflashy suggestion of “deployed cyber defence”, could not generate the required support from senior officials, nor the sense of cool, daring adventure for those involved. At both levels, this is masculinist actionism at work: it is better to be hunting than defending, even if this requires verbal and logical leaps of the imagination.

But ‘hunt forward’ is far from alone. In the article, we analysed the US strategies of ‘persistent engagement’ and ‘defend forward’, suggesting that they offered a more attractive alternative to deterrence due to a complex shifting background of masculine ideals and preferences. The maligned concept of cyber deterrence was seen – in line with feminised tropes – as weak, passive, and reactive, while persistent engagement would ‘take this fight to the enemy’, meaning the United States would not just ‘sit back and take it’.

Another example we discuss is the label of ‘active defence’, which usually refers to a policy wherein many organisations – from the military to government departments to private companies – would be encouraged (or entitled) to act outside their ‘home’ networks, domestic or worldwide. For some, active defence involves tasking non-state actors with ‘hacking back’ after cyberattacks. This strategy repeatedly reaches state and federal levels in the United States, but has so far always been rejected.

Policymakers reject active defence not just because it is a bad idea, administratively speaking, or even because it increases the risks of conflict. At the levels of label and implementation, it fails to find the sweet spot between being sufficiently ‘tech masculine’ to resonate with digital natives and sufficiently ‘military masculine’ to meet the approval of soldiers steeped in ideas of physical bravery and state domination. The concept of active defence goes too far away from military masculinity, undermining the power of the state, in general, and defence and national security, in particular.

While our argument focuses on the United States, there are implications worldwide. The interaction of tech and military masculinities differs in different social contexts, and so the UK’s hunt-forward operations will likely end up sounding – and being used – differently to those of the United States. However, in a year when polls put Donald Trump very close to the US presidency, we should not underestimate the role of

gendered shorthand in shaping cyber strategy. From a White House formerly motivated by the idea of "making the other guy bleed" in cyberspace, in the words of a senior Trump official, the baked-in masculinities of the language and ideas used to describe this digital domain really matter.

- *This article is based on "Masculinist actionism: gender and strategic change in US cyber strategy" in Security Studies and first appeared at Binding Hook.*
- *Featured image: Photo by charlesdeluvio on Unsplash*
- *Please read our comments policy before commenting.*
- *Note: This article gives the views of the author, and not the position of USAPP – American Politics and Policy, nor the London School of Economics.*
- *Shortened URL for this post:* **https://wp.me/p3I2YF-e2U**