THE NATIONAL INTEREST

War Is Still War: Don't Listen to the Cult of Cyber

Brandon Valeriano

May 30th, 2022

There is a false hope for cyberwarfare to be a sanitizer for the practice of war.

Is there some form of cultural attribute, ethos, or collective ideal of like-minded warriors who push for victory in war? Applied to cyber security, what is the culture of the cyber warrior? Such questions go to the heart of cyber warfare, suggesting there is some collective ethos for the state-based hacker.

Culture can be simply defined as the customs and social practices of a collective group. Besides an obvious preference for hoodies, what cultural practices define and distinguish those who will fight the digital battles of the future?

Unfortunately, there is no real culture for the cyber warrior. Rather, there is a consistent ideology and a system of ideals. That ideology believes in technological solutions to human problems and hypes up the impact of cyber action. Like the telegraph, radio, and television before it, computers were thought to revolutionize world politics. And while cyber, like previous technologies, increases the speed of interactions, it does not revolutionize the battlefield. The ideology of cyber hype is a failing practice that represents something of a modern cult.

The Cult of Cyber Warfare

There is an expectation for cyberwarfare to be a sanitizer for the practice of war, making war easier to wage. A great example comes from an early *Star Trek* episode in which two opposing sides simulate battles through a computer, with the loser being lined up for incineration. This was supposedly more humane than prolonged conflict. Absent the horrors of war, conflict continued unimpeded until Captain Kirk saved the day by destroying the war simulators.

The central (forgotten) lesson from this example is that you cannot remove the horrors of war from the practice of violence. War has never gone extinct because it serves as an inefficient solution to the issue of political contestation, or who gets what. Doing this through the computer is no shortcut or replacement.

Even so, the cult of the cyber warrior grew around fear. The technical difference between what scholars mean by culture in military affairs and what makes a cult is, in fact, very negligible. Cults are defined by veneration and dedication to some object or idea, and the blind faith in the transformative power of cyber capabilities reflects this.

We have been here before. For example, the period prior to World War I has been described as the cult of the offensive. The idea that offensive doctrines are superior to defense operations led to overconfidence in offensive plans, which slammed right into the reality of trench warfare and machine guns. We are here once again, with expectations of technologies transforming the battlefield in Ukraine crashing into the reality of bogged down battles aided by light weapons and cheap drones.

The Purpose of Cyberwar

Cyber cultists are still searching for the grand example of success in cyberwar. Yet, there remains no central strategic purpose behind cyber warfare. It's not an effective coercive tactic or a useful form of espionage. Instead, cyberwar is a tool of disruption. Even Russian president Vladimir Putin noted this recently when he complained that "serious attacks [against Russia] were inflicted on the official websites of the authorities. Attempts of illegal penetration into corporate networks of leading Russian companies are also recorded much more often." In the lead up to the Ukraine war, predictions of dramatic "shock and awe" in cyberspace abounded, but there is little to show for it besides "attempts of illegal penetration."

Even demonstrating coordination with battlefield operations seems beyond reach for cyber warriors. Microsoft's special report on Russia's cyber activity in Ukraine did not demonstrate coordination between cyber actions and conventional attacks despite reports to the contrary. The evidence of coordination is noted by pointing out that cyberattacks come after battlefield failures, which is hardly the evidence of complementary cyber activity many had been expecting.

The hope for the cultists is that cyber operations will replace traditional mortars and bombs, lancing out through the fiber cables to strike at the enemy and bend them to the will of the attacker. It is thought that cyber capabilities provide a state with the means to achieve its objectives without firing a shot. The reality is that attackers hardly demonstrate an impact on weakly protected critical infrastructure, let alone the battlefield.

Cyber capabilities mostly make it easier to communicate and organize. The prime example might be GIS Arta, Ukraine's "Uber-like" system of allocated military fires on a selected target. Instead of cyber operations providing a direct path to victory, algorithms rather allocate forces based on distance, readiness, and capability, much like the Uber system does when finding a ride in the middle of New York City. While the GIS Arta system solves one problem by quickly allocating force on a contested battlefield, it also makes the user dependent on the system, creating new vulnerabilities.

The problem with many technologies is that they create new problems while solving other challenges. The internet was created without security in mind; soon, an entire industry was created to solve the problems introduced by the internet. The dominant cultural trait of the cyber warrior is making and solving problems with the same technology.

Those asking why Ukraine did not experience the predicted cyberwar skip the basic question of why we would assume that cyber operations could be leveraged for battlefield effect in the first place. This goes to the heart of the question of the culture of the cyber warrior: those who believe in the ideology of cyberwar expect the battlefield to be transformed by cyber.

Sadly, those with experience in the technology and its uses by governments and militaries will feign shock when the predictions of excited outsiders do not come to fruition. Transformative cyberwar is simply magic, and it is often trumpeted by charlatans. The central cultural trait of the mythical cyber warrior is a belief in magic. There is little difference between Harry Potter's adventures and the fiction of the cyber hacker capable of bringing down countries from their basement. So, do you believe in cyber magic or not?

Brandon Valeriano is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University.