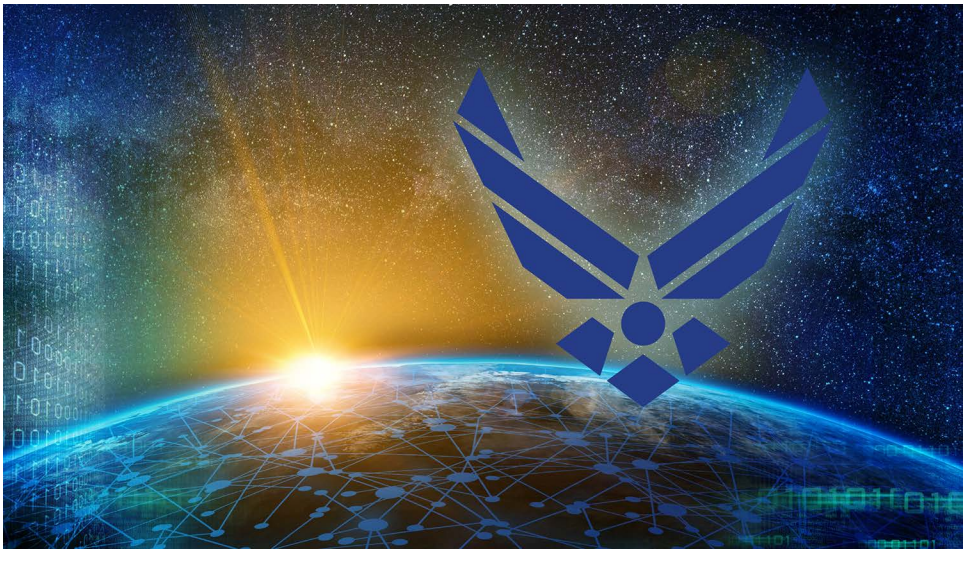
Information Warfare, Cyberspace Objectives, and the US Air Force

Brig Gen Gregory J. Gagnon, USAF

> *Cyberwarfare is an emerging battlefield, and we must take every measure to safeguard our national security secrets and systems. We will make it a priority to develop defensive and offensive cyber capabilities at our U.S. Cyber Command and recruit the best and brightest Americans to serve in this crucial area.*
>
> —White House, 7 January 2017



Good or bad, odd or even, night or day, from a very young age, and throughout our schooling, we are taught through dichotomous logic. It often unconsciously shapes how we perceive the world and impacts our decisions. Before we were the Department of Defense (DOD), we were the Department of War. That dichotomous logic of war or peace often extends unconsciously to America's thinking about defense and security. The *National Defense Strategy* correctly identifies this national cognitive bias. It articulates a need for the DOD and the nation to compete today below the threshold of war to defend and secure US national security objections against adversaries who are actively using all elements of their national power to achieve their desired outcome. Although we use

the term *information warfare*, such activities may be most impactful in times below the threshold of war. In October 2019, the US Air Force established the Sixteenth Air Force, our Information Warfare Numbered Air Force, and in only a short nine months and three days rapidly accelerated this organization from the *initial* operating capability to the Headquarters *full* operating structure by July 2020.

Information warfare is often a debated term; in fact, it currently lacks an approved joint definition. But for the Air Force, we are focusing on information warfare (IW) as activities that synchronize the elements of intelligence, surveillance, and reconnaissance, cyberspace operations, electromagnetic warfare, and information operations to achieve outcomes in times of both war *and* peace. Today, the Air Force describes *information warfare* as "the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior."[1]

As a subset of IW, military activities in cyberspace often receive an increased amount of press. Those not involved in these activities sometimes think these military and security activities are fundamentally different and unique. But when space and cyberspace are thought of as separate and different from other domains of warfare or as separate and different elements of statecraft, our ends can become myopic, disjointed, and suboptimized. The more germane question to consider is how can cyberspace and operations in, through, and from cyberspace support US national interests? Deeper thinking about this issue reveals a strategic opportunity. Unfettered, ubiquitous global access to cyberspace is a national interest for the US, meaning a strategic objective should also be "unrestricted" access to the global network *for other global citizens*. The US Air Force is preparing itself to capitalize on this opportunity.

The Executive Branch issued an executive order on 11 May 2017 "to promote an *open*, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft." The executive order also directed multiple Executive Branch directives to assess cyberspace risk management across the federal government with follow-on requirements to build plans to improve our defensive posture. From a strategy perspective, these defensive actions are intended to deny our adversaries benefits from attacking through diminishing the likelihood of a successful attack operation.

After entering office, the Trump Administration boldly pronounced in its "Making Our Military Strong Again" proclamation that "cyberwarfare is an emerging battlefield, and we must take every measure to safeguard our national security secrets and systems. We will make it a priority to develop defensive and offensive

cyber capabilities at our U.S. Cyber Command."[2] Since then, many organizational changes have occurred within the DOD. Both US Cyber Command (2018) and US Space Command (2019) were elevated to full unified combatant command status to enhance and secure our need for freedom of action in both respective domains. Additionally, services have realigned corresponding capability development organization to meet the expanded organizing, training, and equipping needs.

Adversary attack activity is incentivized by our defensive posture or the lack thereof. The criticality of the internet to our economic well-being is fully documented and widely understood. Equally clear and documented are the cyberspace dependencies laced throughout our critical resources and key infrastructure. By and large, much of our academic writing and policy thinking about cyberspace deterrence has been about deterring adversaries by our own defensive actions. Deterrence outcomes manifest inside a decision-maker's mind. It is a complicated balancing of risk and perceived gain. In this calculus, offensively threatening an adversary is important to incentivize their restraint. An aspect that is less clear to most Americans is how information and offensive cyberspace activities can be used to promote US interests abroad and cause our adversary leadership to have to factor in the threat of a US information attack.

The offensive side of the strategy debate often remains hidden from public discourse. When most think of offensive cyberspace warfare, they think of a Hollywood portrayal of a young man, fueled on energy drinks, wearing a hooded sweatshirt hacking in the midnight hours. Or they might think of today's Russian sponsored third-party internet trolls creating disinformation for others to read and believe. Either way, we inherently assume a dark, pejorative un-American way of statecraft and these dishonest activities should make us uneasy. But what if offensive cyberspace activities could be completely congruent with promoting our foundational ideals—freedom of speech, freedom to assemble, and a commitment to truth and reason?

Using tailored operations actively promoting these foundational ideals, through and from cyberspace, would be very similar to the whole of government approach we used to battle communism during the Cold War. During the Cold War, we pursued a containment strategy against the Soviets. Resident within this approach was an active information component transmitted via Voice of America into the darkest corners of the world. Voice of America news broadcasts were a key tenet in how we countered the Soviet Union's expansionary policies in Eastern Europe with a counterbalancing barrage of freedom of expression and freedom of the press. Equally important to our strategy were approaches designed to hold our adversary's military might at a disadvantage. The Strategic Defense Initiative, which was dubbed "Star Wars," was envisioned to protect the US from Soviet

nuclear forces. From the Soviet perspective, their strategic forces were the key to their stabilizing strength. The DOD and 16th AF's outreach and collaboration with the Department of State's Global Engagement Center is more profound than most would consider due to the change in today's information environment. Our ability to project truth can now be enhanced. For example, changes in the global space market such as SpaceX's desire for true global internet connectivity from micro satellites make this access environment more fertile.

Today's most vexing national security challenges are the expansionary foreign policies of Russia, China and Iran and the threats to our homeland by a nuclear-capable North Korea. At first glance, these problems seem unrelated. But upon deeper analysis they each share similarities. These nondemocratic states are closed information societies with autocratic ruling elite. In each case, the internet and ubiquitous access to information and the expression of ideas are seen as threats. What these ruling elite hold most dear, is their illegitimate right and means to rule. *We, as a nation, should directly hold this at risk.*

Expanding free, unfettered access to all global citizens is in the best interest of the United States. But the value is two-fold. First, it expands the key market and most robust portion of the US national economy. Second, it threatens and holds at risk what our adversaries hold most dear—*information control* necessary to legitimize their autocratic rule. Today, micro technology, space, and cyberspace innovation make this possible. From a whole of government perspective, such an approach might contemplate subsidizing, promoting, and utilizing free global internet access to create greater leverage against autocratic regimes. Fundamentally the concept is to open closed societies via the information domain. The military objective in this approach is develop information access.

Unfortunately, the changing nature of statecraft and warfare is already understood by Russian and Chinese leaders. Both nations are conducting aggressive information statecraft while having weaker conventional forces vis-à-vis the United States. The utility of state power, both hard and soft, is to achieve desired ends. . . both should be used in a complimentary manner. The United States' military traditionally does not successfully use IW to improve its positional advantage in peacetime. In Russian practice, doctrine, and writing, we see Russia actively pursuing activities to exploit perceived vulnerabilities of democratic societies short of armed conflict. Information confrontation or informatsionnoe protivoborstvo (IPb) is not a new strategy for the Russians (previously known as active measures). They divide IPb into two useful subsets—informational-technical (electronic warfare, cyber) and informational-psychological (influence). The key element in the information confrontation strategy is to create confusion and sow doubt in the existence of truth. In Georgia, Ukraine, Western Europe, and the United States, Russia is pur-

suing this approach. Russia integrates IPb at all levels of conflict and statecraft. Russia is playing an offensive game, but what if they also needed to allocate resources to the defense? Internal to Russia, the internet is monitored by the government. Recent 2019 legislation dubbed the "sovereign internet" law gives Russian officials wide-raging powers to restrict traffic. Within Russia this is legal and now accepted. Wisely, Russian critics fear the government is trying to create an internet firewall similar to the one employed by the Chinese Communist Party in China. In both countries, the Western concept of individual rights are subordinated to the state. Exposing their risk may cause adversary leadership to recalculate their current courses of action and dis-incentivize their current behavior.

The core US interest in cyberspace remains freedom. Freedom to access information, freedom to express, and in the virtual world, freedom to assemble. We inherently believe in truth, and that through open debate, truth can be discerned. Americans do not fear facts, but our adversaries do. The larger issue to address is not the application of this idea in times of war; it is to recognize *the true value of this approach is in times of peace and state competition.* The twentieth century's broad lesson is that democratic societies prevail over autocratic states and that people long to be free. This is a founding ideal of America. This ideal remains as valid today as it did in 1776, and I suspect it will still be valid in 2076.

I see US Cyber Command and US Space Command as the key elements in expanding our nation's ability to do the informational-technical. The more important piece for us as a nation is to preemptively agree to speak the truth. The truth that freedom of speech matters, the truth that freedom to assemble matters, and the truth that government censorship and control is wrong. People in Russia and China are not afforded liberty. Short of armed conflict, we can create wonderful dilemmas for adversary leadership. They certainly are not holding back on us.

We should not cede space and cyberspace to our adversaries due to a lack of critical thinking about the advantages they can afford us from an offensive perspective. An American national security objective should enable and provide global, unfettered access to the internet, not just for the US but for the world. America leads the world in both the space and the cyberspace markets. Our nation is a nation of innovators. This is well in the realm of doable, and we are a nation of doers. If our adversaries continue to electronically steal our digital intellectual property, attempt to compromise critical US infrastructure, and further erode our military advantage, playing just defense is proving insufficient. Holding at risk their ability to censor the internet is the right leverage to rebalance the equation. ✪

Brig Gen Gregory J. Gagnon, USAF

Brigadier General Gagnon (BA, Saint Michael's College; MS, Naval Postgraduate School; MA, Air University; MA, National War College) is the director of intelligence for Headquarters Air Combat Command (ACC). In this capacity, he advises the ACC commander on organizing, training, equipping, and maintaining combat-ready intelligence forces for rapid deployment and employment in support of combatant commanders and the National Command Authority.

Notes

1. Headquarters United States Air Force, Program Guidance Letter 19-05, Establishment of the Information Warfare Component Numbered Air Force under Air Combatant Command, 6 September 2019, 5.
2. White House, "National Security & Defense," 7 January 2017, https://www.whitehouse.gov/.