# An Airman's View on Deterrence and Cyberspace

General Jay Raymond

*"Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our federal networks, and attack tools and devices that Americans use every day to communicate and conduct business."*

*– US National Security Strategy, Dec 2017*

*"Russian cyberattacks have targeted the White House, the Joint Staff, the State Department, and our critical infrastructure…Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the U.S. Navy, U.S. partners in the Middle East, major U.S. financial institutions, and a dam just 25 miles north of New York City. And of course, North Korea was responsible for the massive cyberattack on Sony Pictures in 2014. What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk."*

*– Senator John McCain, Jan 2017*

Deterrence, military strategy, and national power are taught at all our United States service academies. As a military officer, you will repeatedly study these subjects as you mature and grow into more senior positions. In this article, I would like to share with you my thoughts on deterrence, and what we have been doing to improve our ability in the Air Force to fly, fight and win–in, thru, and from cyberspace.

From the mid-to-late 80s, my duty was to stand watch in a Minuteman ICBM missile capsule near Grand Forks Air Force Base, North Dakota. Because of this experience,


Gen. John W. "Jay" Raymond is the Commander, Air Force Space Command (Air Forces Strategic-Space) and the Joint Force Space Component Commander, U.S. Strategic Command, Peterson Air Force Base, Colorado. General Raymond is responsible for organizing, training, equipping and maintaining mission-ready space, cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands. He directs USSTRATCOM space forces providing tailored, responsive, theater and global space effects in support of national objectives.

General Raymond was commissioned through the ROTC program at Clemson University in 1984. He has commanded at all levels of Air Force organization. His joint assignments include the Office of the Secretary of Defense, U.S. Strategic Command, Commander, Joint Functional Component Command for Space and currently Commander, Joint Force Space Component Command. Additionally, he served as the Director of Space Forces, as a Colonel, in support of operations Enduring Freedom and Iraqi Freedom at the USCENTCOM CAOC.

I learned early in my career that in the military, every task matters. With this contextual experience of the importance of readiness and lethality firmly engrained in my psyche, I left Grand Forks. One month later, the Berlin Wall fell, the Cold War began to melt, and our nation began to think through the implications of a non-bipolar world. Twenty-three years later, I found myself stationed at U.S. Strategic Command, challenged with a resurgent Russia, and an expanded set of potential adversaries. Deterrence remained a cornerstone of US security, but the range of actors and the complexity of challenges required a re-evaluation of deterrence approaches. Today, I find myself charged with Air Force responsibilities for organizing, training and equipping both space and cyberspace forces. And once again, the complexity and range of actors needed to be deterred have expanded. But as a military officer and a practitioner of national security, one thing has remained constant; peace is best preserved from a position of strength, and military strength is derived from readiness which fuels lethality.

Today's geopolitical environment demands a tailored, flexible, and clear strategy that is communicated, resourced and continuously executed. A good strategy articulates ends and explains the ways and means that instruments of national power are orchestrated to achieve those ends. Good strategy calculates risk and captures opportunities advantageous to our Nation for sustained success.

Deterrence is the cornerstone of our Nation's security strategy. Deterrence occurs in an adversary's decision calculus. It does not manifest itself in isolation within a particular domain of warfare. The decision to not act is a holistic summation of the larger circumstance and environment. Ultimately, if we desire to shape and deter an adversary's behavior in cyberspace, we must address deterrence

from an integrated domain perspective and coherently leverage all elements of our national power to achieve our ends.

A deterrence strategy crafted to deny an adversary the benefit of attack is a necessary first step. The second step is to credibly threaten the imposition of a retaliatory action (i.e., impose cost). Our deterrence strategy should also consider the adversary's perceptions of the cost and benefit of inaction where possible.

For the executive branch, the Department of Homeland Security serves as the lead agency for critical infrastructure and key resource defense. Most recently, in 2017, the federal government added electoral systems to the previous list of 16 critical infrastructure/key resources for protection. For the military, our cyberspace mission is more narrowly focused. We operate Department of Defense (DoD) information systems and networks, and protect and defend them against cyberspace attack. When directed, we further enable our military forces' ability to operate in, thru, and from cyberspace at the time and place of our choosing. This encompasses both defensive and offensive cyberspace operations.

Within the Air Force, we have been aggressively pursuing integrated-domain approaches to fortify our contribution to our Nation's deterrence posture. Well-known is our ability to globally find, fix, target and strike. Less known are the Air Force initiatives in cyberspace. To deny an adversary the benefit of an attack, we have hardened our cyberspace perimeter at the enterprise level, collapsed hundreds of networks into one defendable Air Force Network (AFNET), and built defensive maneuver forces to quickly allocate against emerging threats. At the base level, we are transforming our traditional communications squadrons into cyberspace operations squadrons charged with meeting their senior commander's need to assure and protect the organization's mission.

At most Air Force installations, the Cyberspace Squadron Initiative translates into readiness that rapidly generates air and space power when called upon in support of the Nation. Furthermore, across the Air Force, our Materiel Command has partnered and led the expansion of cybersecurity beyond the traditional desktop and laptop environment onto and into our actual weapons systems, such as aircraft, spacecraft, armaments and supporting network control infrastructure. Our adversaries fear the U.S. Air Force in the air and space; hence we suspect they will seek to ground us before and throughout the fight. Our dependence in the air domain has grown over time. The F-4 Phantom, flown by the Air Force from 1963 until 1996, had only 8 percent of its functions performed by software. In contrast, one of today's fifth-generation fighter aircraft, such as the F-22 Raptor, is 80% dependent on computer technology (Demir 2009). This rapid increase in software reliance on our military weapon systems fuels our warfighting advantage on the battlefield, but it has also increased the criticality of cyberspace assurance. From the factory to the flight line, the Air Force is working to ensure our ability to generate and deliver global vigilance, reach, and power in and through a contested cyberspace

domain. From a defensive perspective, Air Force bases and weapons systems represent critical cyberspace terrain that we are urgently shaping to meet this emergent need.

Today, our AFNET enables the command and control of our force and support operations. But today's AFNET and secure network encumber many of our cyberspace operators with network administration tasks and information technology (IT) provisioning functions. The next step in our transformational journey is to realign these forces and expand our cyberspace defensive maneuver capacity. To achieve this end, the Air Force is shaping its IT provisioning services and IT commodities toward fee-for-service contract models. This approach is designed to allow repositioning of our cyberspace-focused Airmen from provisioning IT and services to defending key cyberspace terrain to enable global Air Force operations. All of these efforts are essential to improve our defensive posture, deny the adversary the benefit of an attack, and ultimately to shape adversary perceptions.

As our National Security Strategy (NSS) states, "The U.S. will deter, defend, and when necessary defeat malicious actors who use cyberspace capabilities against the U.S. When faced with the opportunity to take action against malicious actors in cyberspace, the U.S. will be risk informed, but not risk averse, in considering our options." To support the credibility and lethality necessary for deterrence and to decisively respond if deterrence fails, 29 of 39 Air Force-provided Cyber Mission Force teams have reached full operational capability. All 39 Air Force teams are on track for FOC by June 30, 2018, three months ahead of U.S. Cyber Command's (USCYBERCOM) target date. These units, in combination with our sister service teams, will provide USCYBERCOM 133 cyber teams comprised of roughly 6,200 personnel.

Like the missile forces of yesterday and today, our cyberspace assets must train, stay vigilant, and be ready. Their readiness incentivizes adversary restraint by signaling our ability to deny benefit and impose cost thus enhancing deterrence. In August 2017, the President directed USCYBERCOM be elevated to a full combatant command. Active planning to meet this direction is currently underway within the DoD, as USCYBERCOM prepares for full-spectrum military cyberspace operations to ensure US and Allied freedom of action in cyberspace. This further signals US commitment to provide our freedom of action in, thru and from the domain to both Allies and potential adversaries.

The NSS makes clear our intent to protect critical infrastructure and deter and disrupt malicious cyber actors, but in the 21st century, no domain can be understood in isolation. Our ability to deter action in air, land, sea, space, and cyberspace is a manifestation of the collective strength we present across all domains. Conversely, a weakness in any domain undercuts our readiness, hamstrings our lethality and erodes our credibility to deter. America's Airmen represent critical threads in the fabric of our Nation's integrated deterrence strategy. Whether on a keyboard, in a cockpit, or deep in a silo, America's Air Force stands ready to deliver Global Vigilance, Global Reach and Global Power, in, thru and from air, space, and cyberspace.