175 NETWORK WARFARE SQUADRON

MISSION
175 Information Operations Squadron provides information operations support in the form of network warfare operations to the U.S. Air Force and other locations as assigned through integrated planning, employment and assessment of joint information operations requirements and capabilities. Officers: 22 Enlisted: 37

LINEAGE
175 Information Operations Squadron
175 Network Warfare Squadron

STATIONS
Warfield Air National Guard Base, Middle River, MD

ASSIGNMENTS

COMMANDERS
Col Timothy Evans

HONORS
Service Streamers

Campaign Streamers

Armed Forces Expeditionary Streamers

Decorations

EMBLEM

On a disc Azure, a diamond throughout Gules, fimbriated by four lightning bolts, charged with a terrestrial globe Or, landmasses and grid lines Sable, in chief to dexter three bend sinisterwise mullets Argent, all within a narrow border Yellow. Attached below the disc, a Scarlet scroll edged with a narrow Yellow border inscribed "175 INFO OPS SQ" in Yellow letters. Ultramarine blue and Air Force yellow are the Air Force colors. Blue alludes to the sky, the primary theater of Air Force operations. Yellow refers to the sun and the excellence required of Air Force personnel. The globe symbolizes the cyberspace domain in which the unit fights. The three stars represent the belt in the constellation known as Orion, the hunter. Hunting is the major activity of the unit's network warfare mission. The three stars also suggest the four three-letter agencies to which the unit provides support, including NSA, CIA, DHS and DIA. The lightning bolt bordered diamond depicts the electronic threats that exist within the global cyberspace domain.

MOTTO

NICKNAME

OPERATIONS

In 2009, the 175th Information Operations Squadron was redesignated as the 175th Network Warfare Squadron, without a change in location or mission. The 175th Network Warfare Squadron continued to support U.S. Air Force forensic analysis of malicious code and intrusion vectors and performed technical research and analysis on cyber infrastructure issues related to emerging technologies.

In march, Air Force Secretary michael donley announced the creation Of two new Air Guard information-operations squadrons, one in California and one in Washington state. In addition, he said, the Air Guard would be expanding the Maryland Guard's 175th Network Warfare Squadron noted for its work with the National Security Agency. These new additions will be "cyber hunter squadrons," part of a fresh and more aggressive approach to defending military networks called "active defense." Their job will be to monitor networks for intrusions and unauthorized users, to analyze what they find and develop countermeasures, says Lt. Col. Sean Kelley, the chief of the Air Guard's Cyberwarfare and Information Operations Division. The central tenet of their mission is "preemptive defense—go out and find threats before they find you," Kelley says. The units will include intelligence specialists whose job is to uncover information about emerging

cyber threats, and cyber forensic experts who will analyze threats and try to track them back to their origins. The aim of this cyber sleuthing is "mission assurance," eliminating threats and keeping networks running so they can carry out military missions, Kelley says. These new units are just the beginning. "If the Air Force portfolio was the stock market, I would invest in cyber," Lt. Gen. Harry M. Wyatt III, the Air Guard director, told a gathering of defense experts at the Center for Strategic and International Studies. Faced with a defense budget that could cut nearly 200 aircraft from the Air Guard fleet by 2017, Wyatt said the Air Guard "is shifting from a platform-based construct of the past to a capabilities-based force. Of our 106,700 Air National Guardsmen right now, close to 9,000 are already involved in cyber." And that number will be growing. "What we're looking at is a global cyber arms race," said Rear Adm. Samuel Cox, the intelligence chief at the U. S. Cyber Command, told a conference in Washington, D.C., in April. "It's not proceeding at a leisurely or even a linear fashion, but in fact is accelerating." The cyber threat endangers national security, public safety and the U. S. economy, he said. In March, Cox's boss, Gen. Keith Alexander, the chief of the U.S. Cyber Command, reported to House and Senate committees that the U.S. intelligence community now ranks cyber threats "just behind terrorism and proliferation in its list of the biggest challenges facing our nation." And the threat isn't just aimed at the military. "We are also increasingly concerned about the threat to our defense industrial base and the nation's critical infrastructure," said Madelyn Creedon, the assistant defense secretary for global strategic affairs. "We have seen the loss of significant amounts of intellectual property and sensitive defense information that reside on, or transit defense industrial base systems" she told the House Subcommittee on Emerging Threats and Capabilities. Part of the problem is cyber criminals, who steal data that they can sell, Alexander told lawmakers. But in addition to criminals, "several nations have turned their resources and power against us." Alexander didn't name names, but China, Russia and increasingly Iran have emerged as cyber concerns. Still, it remains unclear what role the U.S. military should play in defending U.S. companies and critical infrastructure against cyber attackers. Many in the military are reluctant to assume responsibility for defending nonmilitary cyberspace, in large part because there are long-standing legal restrictions against military involvement in domestic intelligence gathering and law enforcement. "We believe strongly in a whole-of government approach to cybersecurity," Creedon told House lawmakers. That is, the military should work closely with the departments of Homeland Security, Justice, State, Treasury, Commerce and other agencies on cyber defense. The Defense Department spends $37 billion a year on information technology and of that, $3.4 billion goes into cybersecurity, says Pentagon chief information officer Teresa Takai. By contrast, the Department of Homeland Security, the lead agency for protecting U.S. critical infrastructure, has budgeted just $1.2 billion for cyber defense in 2013. "We should not kid ourselves," said Rep. Mac Thornberry, R-Texas, the chairman of the emerging threats subcommittee. "The American people expect the Department of Defense to defend the country in whatever domain it is attacked." Alexander seems willing to take on that mission. "I think in extremis the Defense Department would be the natural ones to defend the country," he told Thornberry. "I believe within the administration there's general agreement that that is correct. The issue is, what are those circumstances? And how do we do it? A number of U.S. laws forbid the military to spy on "United States persons" in the United States, among them the Foreign Intelligence Surveillance Act, the Fourth Amendment to The Constitution and the Posse

Comitatus Act. “U.S. persons” include U.S. citizens, legal aliens, associations and U. S. corporations.

The 175th Network Warfare Squadron continued to support U.S. Air Force forensic analysis of malicious code and intrusion vectors and performed technical research and analysis on cyber infrastructure issues related to emerging technologies. The squadron also provided language support to multiple U.S. Air Force analytical efforts. In addition, the unit completed acquisition of hardware and software of the squadron’s Digital Network Operations Range, providing training resources in support of the Air Force mission. The squadron also provided language support to multiple U.S. Air Force analytical efforts. In addition, the unit completed acquisition of hardware and software and full installation of the squadron’s Digital Network Operations Range, providing training resources in support of the Air Force mission.

The Air Guard leads among reserve forces in developing offensive cyber capabilities. It operates two 100-person squadrons that are capable of launching cyber attacks. They’re Maryland’s 175th Network Warfare Squadron and Delaware’s 166th Network Warfare Squadron. Both squadrons support the National Security Agency, but Guard officials in Delaware and Maryland declined to discuss what the units do. As cyber operations and units expand, the active-component services are struggling to attract and retain qualified cyber troops. But that’s proving to be less of a problem for the Guard. In an address at a CyberFutures Conference in March, Gen. William Shelton, the chief of the Air Force Space Command, called the shortage of cyber recruits for the Air Force “a serious national security issue.” Shelton said far too few U.S. college graduates now are earning technical degrees. Of those who do, too many are foreign nationals who are ineligible to work in U.S. national security. And too many others “aren’t the kind of folks that would necessarily take well to military life,” he said. Pay is another problem. “There’s no way that the military can compete with civilian salaries” for cyber professionals, said Wyatt, the Air Guard director. But pay disparity creates opportunities for the Guard. By joining the Guard, cyberwarriors can keep their high-paying civilian jobs and still serve in the military. That formula seems to be working. The authorized personnel end-strength of Rhode Island’s 102nd is 50 airmen, but “we’re currently stacked at 58,” said Marshall, the operations officer. In Washington state, where the 143rd Information Operations Squadron is being created from a combat communications squadron, “we’re demographically blessed,” says Dravis, the wing commander. The 143rd’s headquarters sits about two miles east of Interstate 5, which runs from Canada to Mexico along the West Coast. In western Washington, the I-5 corridor is dotted with high-tech industries—Microsoft, Cisco, Boeing, T-Mobile, supercomputer-maker Cray and dozens of software companies. “We pull extensively from them,” Dravis says. “We have significant experience levels walking into our units.” The Los Angeles area is another “hotbed of cybertech,” says Col.Stephen Beck, commander of the California Air Guard’s 162nd Combat Communications Group. The group’s new 261st Information Operations Squadron is based in Van Nuys, just north of L.A. In addition to numerous high-tech companies, many with ties to the military, the area has “tons of universities and two dozen cyber-research centers, all within an hour or two drive,” Beck says. Similar demographics exist for the 175th in Maryland. As it expands, it expects to draw from high-tech companies clustered around Washington, D. C., and Baltimore. The locations are no coincidence. The three units were selected for cyber missions because of their proximity to cyber-

savvy populations, Wyatt said. But proximity isn't always essential. "We've got a cyberwarrior in Washington state," Wyatt said, "who, on drill weekends, on his own dime, flies to the east coast to Fort Meade to do battle with folks worldwide." 2012

USAF Unit Histories
Created: 26 Dec 2010
Updated: 18 Apr 2021

Sources
Air Force Historical Research Agency. U.S. Air Force. Maxwell AFB, AL.
The Institute of Heraldry. U.S. Army. Fort Belvoir, VA.
Air Force News. Air Force Public Affairs Agency.