U.S. Navy's fourth Mobile User Objective System communications satellite will bring advanced, new global communications capabilities to mobile military forces (Courtesy United Launch Alliance/U.S. Navy)

Beyond the Build

How the Component Commands Support the U.S. Cyber Command Vision

Compiled by the U.S. Cyber Command Combined Action Group

Networked technology is transforming society. That transformation has come with significant change to war and the military art. Until recently, cyber considerations rarely extended beyond the computers and cables that supported kinetic warfighting functions. The natural domains—land, sea, air, and space—dominated the planning and conduct of operations, while the risks entailed in using cyberspace for military purposes went largely unrecognized. Today, cyberspace ranks as its own warfighting domain—one that intersects the four natural domains.

Cyberspace operations demand unprecedented degrees of collaboration, which the U.S. Government must approach holistically—leveraging resources and expertise from industry, academia, and state/local governments, as well as allied and coalition partners. U.S. Cyber Command (USCYBERCOM) works as a subordinate, unified command under U.S. Strategic Command (USSTRATCOM) to conduct the full scope of cyberspace operations. These have three distinct mission areas: to secure, operate, and defend the Department of Defense Information Network (DODIN); to provide combatant command support; and to defend the nation against strategic cyber attack. USCYBERCOM is building the cyberspace operations force of tomorrow, and

looking beyond that build to how the command will operate with mission partners in this dynamic and contested space.

USCYBERCOM and its components act to help the joint force operate globally with speed, flexibility, and persistence. USCYBERCOM headquarters focuses on defining and achieving strategic objectives and has delegated operational-level cyber mission areas to three types of headquarters. The first of these is the Cyber National Mission Force (CNMF), which defends the United States and its interests against strategic cyber attacks. The second type of headquarters comprises four distinct joint force headquarters (JFHQs) in addition to Coast Guard Cyber Command (CGCYBER) to support the geographic and functional combatant commands across the globe. The standup of a JFHQ-Cyber by each of the USCYBERCOM Service cyber components—Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Marine Corps Cyberspace Command (MARFORCYBER), and Air Forces Cyber (AFCYBER)—constitutes a vital first step to integrating cyberspace operations to deliver effects in support of combatant commanders. The third type of JFHQs and newest of USCYBERCOM's operational commands, JFHQ-DODIN, provides unity of command and unity of effort to secure, operate, and defend the DODIN.

Each of these components and its respective joint force headquarters have a vital role to play as we finish building the Cyber Mission Force (CMF) and work together to bring the USCYBERCOM Vision to fruition. The main elements of this vision serve to organize and guide their efforts (see the interview with Admiral Michael S. Rogers, USN, in this edition of *Joint Force Quarterly*). *JFQ* asked each of the component commands to summarize its efforts on behalf of the collective enterprise toward implementing the vision. This article represents a compendium of these contributions, organized around the main elements of the vision's intent.

Motivated by Mission

Each of the Service components contributes to USCYBERCOM missions by providing an array of cyber forces and capabilities in order to defend DOD Information Networks, bolster the capabilities of combatant commands, and strengthen our nation's ability to withstand and respond to cyber attacks of significant consequence. Each component also fulfills Service-specific requirements in cyberspace, which are correlated with and unique to the individual Service's role in the domain of land, sea, air, or space.

ARCYBER's three priorities are to operationalize cyberspace operations to support combatant and Army commands at echelon; pursue a more defensible network; and organize, man, train, and equip ready cyber forces. These priorities strengthen both joint and Army cyber capabilities, enable ground forces to continue their dominance in the land domain, and support the Army's top goal of readiness to fulfill its primary mission to win in ground combat. ARCYBER supports Army tactical forces and has made delivering cyberspace operations capabilities to Army corps and below a major focus. The integration of networks, systems, and data has delivered unprecedented awareness and warfighting capability to the tactical edge—to the point that it is now a dependency, which by extension makes it a vulnerability that must be protected.

FLTCYBER's missions align to those of USCYBERCOM. They are to operate Navy networks as a warfighting platform, produce signals intelligence, deliver warfighting effects through cyberspace, create shared cyber situational awareness, and establish and mature the Navy's cyber mission forces. FLTCYBER conducts operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and joint freedom of action and decision superiority while denying the same to the adversary. Achieving this requires FLTCYBER to operate and defend the Navy's networks and shore-to-ship communications including Nuclear Command and Control Communications (NC3), plan for and operate Navy spacecraft, oversee information operations, coordinate Navy electronic warfare, and plan and direct operations under USCYBERCOM.

The Coast Guard focuses on three strategic priorities in the cyber domain: defending cyberspace, enabling operations, and protecting infrastructure. CGCYBER ensures the security and resiliency of Coast Guard information technology systems and networks to ensure the full scope of Coast Guard capabilities. Maritime critical infrastructure and the Maritime Transportation System (MTS) are vital to our economy, national security, and national defense. The MTS includes ocean carriers, coastwise shipping along our shores, the Western rivers and Great Lakes, and the Nation's ports and terminals. Cyber systems not only enable the MTS to operate with unprecedented speed and efficiency, but also create potential vulnerabilities. This technology is inextricably linked with all aspects of Coast Guard operations. As the maritime transportation Sector Specific Agency (as defined by the National Infrastructure Protection Plan), the Coast Guard provides the unity of effort required to protect maritime critical infrastructure from attacks, accidents, and disasters.

Along similar lines, MARFORCYBER is shaping the tools, doctrine, processes, and capabilities to ensure Marine cyber mission teams provide effective support to USCYBERCOM and the joint force, while also ensuring Marine Air Ground Task Forces (MAGTFs) achieve victory on the modern battlefield. AFCYBER's mission statement—"Fly, Fight and Win In, Through, and From Cyberspace"—captures a breadth of responsibilities to include extending cyber capabilities to the tactical edge of the battlefield.

Each Service, as part of the broader joint force team, is responsible for protecting its Service-specific cyber network (for example, LandWarNet, AFNET, Marine Corps Enterprise Network, Navy Marine Corps Intranet) to ensure its ability to detect, mitigate, and defeat advanced persistent threats capable of compromising the network and DODIN itself. The scale of this mission cannot

U.S. Army Chief of Staff General Mark Milley watches officers from Army Cyber Institute demonstrate Cyber Capability Rifle during 2015 Association of the U.S. Army annual meeting, Washington, DC (U.S. Army/Chuck Burden)

be overstated. The Navy Marine Corps Intranet, for instance, consists of more than 500,000 end user devices, approximately 75,000 networked devices, and nearly 45,000 applications and systems across three security enclaves.

Each Service cyber component focuses on configuring and operating layered defense-in-depth capabilities to prevent malicious actors from gaining access to Service-specific networks. This is an enterprise-wide effort in which the components work in collaboration with their parent Services, USCYBERCOM, JFHQ-DODIN, the Defense Information Systems Agency (DISA), and the National Security Agency (NSA). The Service cyber components function at the operational and tactical levels of this domain and rely on JFHQ-DODIN to ensure lateral coordination, information-sharing, and synchronization—ensuring the unity of effort for the operation and defense of the entire DOD information environment.

With its standup in 2010, USCYBERCOM rapidly focused on providing mission assurance for the DOD information network, deterring or defeating strategic threats to U.S. interests and infrastructure, and supporting joint force commander objectives. While responding to evolving threats, a new need surfaced for an agile force ready to engage adversaries in the tactical cyber fight when directed by the President. This force gathered talent from across the DOD and Intelligence Community to build teams with the capabilities and understanding needed to collaborate with foreign and domestic partners engaged in the same mission. Since 2013, the Cyber National Mission Force has developed into a highly proficient and agile force operating across the spectrum of conflict in cyberspace, with appreciation for the effects that cyberspace operations have on the physical warfighting domains.

The CNMF is a joint force of military and civilian members from the Army, Marine Corps, Navy, Air Force, Coast Guard, and Intelligence Community. It will comprise 39 teams and nearly 2,000 personnel spread over four locations. The force consists of three types of maneuver elements, each with a unique and specified mission. National Cyber Protection Teams (NCPTs) are defensive elements working within DOD networks and, when authorized, outside DOD networks, identifying and mitigating vulnerabilities, assessing threat presence and activities, and responding to adversary actions. National Mission Teams are maneuver elements conducting on-network operations in neutral and adversary territory,

looking for indications and warning of adversary cyber activities, and enabling cyber effects when authorized and directed. National Support Teams are analytic elements providing planning, development, and technical support to National CPTs and Mission Teams. The creation of teams with distinct, mutually reinforcing missions presents commanders with forces capable of confronting and defeating a growing and creative series of threats.

Powered Through Partnerships

Cyberspace is the quintessential collaborative environment where teaming with partners inside and outside government will determine how successful we are in defending the nation. Adversaries' targeting of both public and private sectors underlines the necessity of building strong partnerships.

The Army's cyber community includes a triad of three critical partners—ARCYBER, the new Cyber Center of Excellence (CCOE), and the Army Cyber Institute (ACI)—that collaborates to advance the state of the art in cyber operations and work with the larger Army to share cyber-related advances. The CCOE, located at Fort Gordon, Georgia, is ARCYBER's institutional cyber component and is developing its structure, curriculum, and methods to meet future challenges and mission requirements. The ACI, located at West Point, is the primary cyber innovation agent and bridge builder, responsible for developing partnerships between the Army, academia, government, and industry, while providing insight into future cyber challenges through interdisciplinary analysis on strategic cyber initiatives and programs. ARCYBER, CCOE, and ACI work together to develop high-payoff external partnerships across the interagency community, U.S. Government, and national and international cyber communities of interest.

FLTCYBER, as the Navy's warfighting fleet in cyberspace, maintains partnerships to leverage their strengths and maintain focus on the missions. The Deputy Chief of Naval Operations for Information Dominance prioritizes and allocates resources; Navy Information Dominance Forces man, train, and equip forces; Space and Naval Warfare Systems Command, as the technical authority, delivers and sustains capabilities and systems. FLTCYBER's operational partners execute the Navy's mission every day to reduce the network attack surface, educate both commanders and users, modernize unsupported systems, improve patch maintenance and configuration control, inspect compliance, and reduce our collective risk.

The Coast Guard has a unique set of authorities to conduct cyber operations in support of its missions. It works with partners across the Federal Government; in foreign governments; at the state, local, tribal, and territorial levels; and in the private sector. At the Federal level, the Coast Guard aligns capabilities and coordinates operations with the Department of Homeland Security (DHS) and works with the Federal Bureau of Investigation (FBI), the NSA, USCYBERCOM, and other departments and agencies. The Coast Guard trains its operational personnel to the applicable standards of all partners, and where appropriate, integrates its cyber personnel into partner agencies to enhance coordination. The Coast Guard also fosters relations with private sector members of the Marine Transportation System to better understand its vulnerabilities and support their cybersecurity efforts.

For AFCYBER, 25th Air Force (25 AF) continues to be a critical strategic partner across all missions because success in today's cyberspace operations hinges on the effectiveness of cyber intelligence, surveillance, and reconnaissance (ISR) to meet warfighter requirements. AFCYBER and 25 AF have partnered on the Cyber–ISR–Electronic Warfare Mission Integration Team initiative aimed at leveraging their respective unique capabilities to develop and field innovative, multidomain solutions in support of combatant and air component commanders' urgent needs.

The CNMF plans, directs, and synchronizes full-spectrum cyberspace operations to be prepared to defend the U.S. homeland and vital interests from disruptive or destructive cyber attacks of significant consequence. Headquartered at Fort Meade, Maryland, it has forces in Georgia, Texas, and Hawaii, and engages with partners around the world. It synchronizes efforts across disparate time zones and optimizes the balance between on-site and remote operations to achieve lasting effects. The success of the CNMF mission relies on establishing and nurturing partnerships, including relationships with the NSA, DOD, and Intelligence Community, to widen its awareness and capacity to deliver effects. The CNMF is strengthening partnerships with DHS and FBI to enable future operational success and expanding its partnerships to include other Federal agencies, industry, academia, and the international sphere.

The cyberspace domain is primarily owned and operated by private industry and thus the ability to collaborate with industry partners benefits the Nation's cybersecurity posture. The Army has hosted multiple industry events including a Joint Service Academy Cyber Summit with C-suite executives from industry and a twice a year Cyber Talks event held at the National Defense University that convenes innovators from industry and inside DOD to share ideas. FLTCYBER leverages industry leaders to help defend the network. Experts from the Navy have worked with industry to use data analytics and create new techniques that better detect malicious activity. In the past, FLTCYBER has also teamed with industry to conduct defensive cyber operations on Navy networks. In addition to daily interaction with industry partners, AFCYBER has developed Cooperative Research and Development agreements with cybersecurity, telecommunications, and cleared defense contractors (comprising at least 28 industry partners) to collaborate on innovative technologies and concepts, advance the science and technology of cyberspace operations, and exchange best practices. JFHQ-DODIN continues to partner with industry to include exploring cooperative research and development efforts and academic outreach. Additionally, it leverages DISA's long-established industry, academia, and research and development efforts to improve its approach for shaping DODIN operations and defense.

Local partnerships also exist. The Army has a relationship with Augusta, Georgia, and is building strong ties in Atlanta to create a public-private "center of gravity" in support of cyberspace operations, workforce development, and technical innovation. AFCYBER has a long-standing relationship with San Antonio, Texas (referred to as "Cyber City USA"), which includes civic-leader engagements to swap lessons related to cybersecurity and support programs to engage young students. The Air Force Association's "CyberPatriot" STEM (science, technology, enginneering, and mathematics) initiative sees Airmen mentor cyber teams as part of a nationwide competition involving over 12,000 primary and secondary school students.

Each of the Service components has ties to academia. CGCYBER is leveraging its relationship with the U.S. Coast Guard Academy and industry to capitalize on its knowledge of trends in cyberspace. MARFORCYBER is leveraging partnerships with The Johns Hopkins University, Carnegie Mellon University, and Naval Postgraduate School (NPS) to build knowledge, skills, and experience in a continuous cycle of professional development. ARCYBER has championed scholarships and collaborative research with top-tier academic institutions such as The Johns Hopkins University, University of Maryland, Carnegie Mellon University, Virginia Tech, and Georgia Tech. AFCYBER leverages expertise from the Air Force Research Laboratory, MIT Lincoln Laboratory, MITRE, Air Force Institute of Technology, National Air and Space Intelligence Center, Air University, and the U.S. Air Force Academy, as well as academia and industry to meet growing joint warfighter needs.

FLTCYBER is well integrated into academia, in particular NPS, where the FLTCYBER commander serves as the sponsor for the computer science, cyber systems and operations, and master of science in applied cyber operations curricula. These programs deliver graduates who meet the evolving operational needs of the Navy and other Services. NPS offers outstanding graduate degree programs that contribute to the development of officers and enlisted personnel. These programs include electrical and computer engineering, computer science, cyber systems operations, applied mathematics, operations analysis, and defense analysis. The Naval War College, which hosts a Center for Cyber Conflict Studies, is incorporating cyber into its strategic and operational level of war courses at both intermediate and senior graduate course levels, and has emphasized cyber in its wargaming role. FLTCYBER partners with the U.S. Naval Academy's Center for Cyber Security Studies, as well as offering summer training opportunities to Academy and Reserve Officer Training Course (ROTC) Midshipmen. The Navy is also working with the Johns Hopkins Applied Physics Laboratory, Carnegie Mellon, Penn State, University of Texas, MIT Lincoln Laboratory, and University of Hawaii. In addition, FLTCYBER has partnered with the University of Maryland, Baltimore Campus, to offer internships for recruiting skilled civilian and military cyber workforce professionals.

Oriented Toward Outcomes

The Commander's Vision for USCYBERCOM and its operational components calls for integrating cyber into new ways of defending, fighting, and partnering. To execute their missions, USCYBERCOM and its components must turn strategy and plans into operational outcomes. This requires commitment to an operational mindset whereby networks and cyber capabilities are not administered but rather led by commanders who understand they are always in real or imminent contact with adversaries.

More than 5 years ago, the Navy created a fundamental shift from "Information in Warfare to Information as Warfare," and has assimilated this operational mindset. The Navy recognizes that freedom of action in cyberspace is essential to maritime operations. From satellites orbiting above the Earth to the "Silent Service" below the seas—and everything in between—the Navy depends on cyberspace for assured command and control, integrated fires, battlespace awareness/intelligence, maneuver, protection, and sustainment. Understanding that the "cyber platform" extends beyond traditional IT and business systems, the Navy is extending its cybersecurity apparatus to all networked capabilities including warfighting control and combat systems, combat support, and other information systems while strengthening authority and accountability. Task Force Cyber Awakening (TFCA) was established to improve the Navy's cybersecurity posture based on procedures devised for Operation *Rolling Tide*, the response to incidents involving the Navy Marine Corps Intranet in 2013. The Navy realized it needed the ability to "maneuver" the network during cyber incidents. TFCA addresses organizational, financial, cultural, workforce, and technical issues. It includes development of a cyber resiliency plan—the CYBERSAFE program—that focuses on assuring the survivability of critical capabilities.

The Army Chief of Staff challenged ARCYBER to demonstrate tactical cyber integration at Brigade Combat Team–level home-station training and at the Combat Training Centers. Lessons from these pilots are informing the Army's employment and integration of cyberspace capabilities and the convergence of information operations and electronic warfare. The Army will use exercises to inform the concepts, organizations, and capabilities needed to support ground forces. These experimental efforts are helping to create a cultural shift in which innovators, experimenters, and creative thinkers are valued despite drawdowns and resource constraints. These efforts also teach operational forces how to integrate cyber/electronic warfare capabilities into their traditional missions, how to defend their networks, and how to operate under degraded network conditions.

In the same manner with which the Marines employ combined arms to conduct maneuver warfare, MARFORCYBER is integrating and synchronizing the employment of offensive and defensive cyberspace capabilities to protect Marine Corps networks. Operating and defending these networks are as critical to the Corps as securing command posts and combat operations

centers. In January 2015, then-Commandant Joseph Dunford directed integration of cyberspace operations using warfighting principles to increase the MAGTF capacity and capability to operate in and exploit the cyberspace domain. To achieve this end, MARFORCYBER has begun to unify its networks, adapt its manpower model to serve the unique requirements of the cyber domain, define standards for a sustainable cyber readiness posture, and reduce acquisition times to better equip forces with the tools they need to outpace the adversary.

AFCYBER's overhauled command and control structure has been at the center of transforming what was previously a reactive, maintenance-based planning approach to a more operationally focused strategy, plans, and execution process. Built around the joint planning process and modeled after an air operations center organization, Air Forces Cyber now produces daily cyber tasking orders that direct units in the field that perform the full spectrum of cyber operations. These operations include over 50 defensive cyber missions per day to defend key cyber terrain in support of combatant and air component commanders.

To maximize the combat capabilities of its existing cyberspace operations forces, AFCYBER established a new force-employment strategy by designating cyber "force packages" and synchronizing them in "vulnerability windows." Like joint force employment in traditional combat operations, these concepts allow the decomposition of existing and emerging cyber capabilities into smaller, more flexible, and consistent units of employment. The result has been simultaneous versus serial actions, compressed execution timelines, and less capability "left on the ramp." Two years ago, AFCYBER was able to conduct a few named operations simultaneously in defense of AFNET and key cyber terrain. Today, the same teams are executing more than 15 named cyberspace defensive operations at once across the AFNET, as well as providing direct support across the full spectrum of cyberspace operations to combatant and air component commanders around the world. Realizing the need to operationalize training, AFCYBER also mirrored cyber operations training based on lessons shared by its counterparts in air and space operations and leveraged the mission qualifications process to ensure cyberspace operators meet mission-ready qualification standards.

U.S. Navy's fourth Mobile User Objective System communications satellite, encapsulated in 5-meter payload fairing, lifts off from Space Launch Complex-41, September 2, 2015 (Courtesy United Launch Alliance/U.S. Navy)

Cyberspace operators from across all the Services participate in USCYBERCOM events such as CYBER FLAG, in addition to Service-specific exercises such as the Air Force Warfare Center's RED FLAG, to hone skills through real-world, force-on-force exercises that integrate cyber capabilities in a live-training environment. These simulations are accelerating the development and fielding of new tactics, techniques, and procedures, and complement efforts to integrate cyber effects with both kinetic and nonkinetic operations across multiple warfighting domains.

The CNMF operates at the tip of the cyber spear, turning USCYBERCOM operational imperatives into executable actions. CNMF teams work together to achieve lasting effects on the enemy: offense informs defense, defense enables offense. As such, the CNMF is poised to deliver a wide range of response options tailored to specific cyber actors and

scenarios. It provides opportunities for its people to grow as members of an operational force and empowers them as leaders who understand technical solutions and inherent risks while being able to communicate with nontechnical senior military and policy leaders. Developing leaders capable of directing cyber operations integrates cyber as a tool in the greater mission to protect national security.

Completing the Build

The Commander's Vision for USCYBERCOM and its operational components calls for accelerating full-spectrum capacity and capability development to give commanders and policymakers the options they need to execute full-spectrum operations. Generating the DOD cyber capability and capacity falls to the Service cyber components with their authorities to man, train, and equip the force.

Each of the Service cyber components is building maneuver elements for the Cyber Mission Force by manning, training, and certifying teams to USCYBERCOM standards. Over the past 2 years, the Army has begun aligning command and control by assigning the Network Enterprise Technology Command to Army Cyber Command and building its Active Component CMF with the goal of having all 41 Army CMF teams on track for full operational capability no later than 2018. Reserve Component forces are an essential part of the Army's cyberspace force, and ARCYBER is also building 21 additional CPTs, 11 in the Army National Guard and 10 in the Army Reserve. To help meet the Army's demand for cyberspace talent, in September 2014 the Army created its first new career branch in nearly 30 years—the Cyber Branch and Career Management Field—to manage cyber talent for the Service and allow career-long professional development. Since September 2014, the Army has handpicked approximately 300 Soldiers from across the force to serve as the first cohort of Cyber Branch officers from lieutenant to colonel, and partnered with ROTC, West Point, and the Officer Candidate School to provide a continual flow of fresh talent. The Cyber Center of Excellence created the first-ever Cyber Basic Officer Leader Course less than 10 months after the branch was formed.

The Navy is on course to have personnel assigned for all 40 Navy-sourced CMF teams in 2016 with full operational capability in the following year. Additionally, by 2018, 298 cyber Reserve billets will also augment the Cyber Force manning plan. The Navy has made establishing and maturing its Cyber Mission Force a top priority. Working with the University of Maryland Center for the Advanced Study of Language, FLTCYBER is developing a Cyber Aptitude and Talent Assessment that will identify talent across the spectrum of technology, analytic capability, and ingenuity. In an effort to meet the growing demand, the Navy is creating ways to better assess, track, and manage cyber talent in the workforce.

FLTCYBER has several efforts under way to identify individuals with critical cyber warfare skill sets by building awareness of Navy cyberspace operations and associated career options. The U.S. Naval Academy established a summer intern program with Task Force 1090, Navy Cyber Warfare Development Group, enabling Midshipmen to gain exposure to a wide range of cyber operations over a 6-week period as part of their summer training. A similar program was established for Naval ROTC Midshipmen with computer-related curricula that allow them to work with Task Force 1020, Navy Cyberspace Defense Operations Command, for their first class summer cruise.

The Air Force will contribute nearly 2,000 Airmen to support the joint cyber force. To meet the CMF's growing requirements, the Air Force has restructured and expanded its training and force development programs, nearly quadrupling the rate at which cyberspace operators and intelligence specialists qualify to join Air Force cyber teams in support of the CMF. Likewise, long-standing cyber programs such as the Air Force Institute of Technology as well as new ones such as the Air Force Academy's Cyber Innovation Center are exposing the next generation of innovative leaders to technical, policy, and operational concepts to prepare them for cyberspace operations. AFCYBER leverages traditional Reservists, Air Reserve Technicians, and Air National Guardsmen across the command to meet its warfighting commitments. These Total Force members meet the same demanding standards and serve alongside their Active-duty counterparts.

Like the Army, the Air Force instituted a new cyberspace officer career field specific to Cyberspace Warfare Operations to develop Airmen with the requisite skills and expertise to meet the Nation's emerging needs. The 2013 standup of a Cyber Weapons Instructor Course at the Air Force Warfare Center was a milestone on the way toward normalizing cyberspace operations in support of combatant and air component commanders by focusing on the tactical employment of these emerging capabilities. In addition, a Cyber Intermediate Leadership program was developed to ensure cyber operators and intelligence officers have the right professional growth opportunities in key command and operational positions. Recently, AFCYBER established a Ready Cyber Crew program to ensure all cyberspace operators receive the right amount and type of continuation training to maximize their combat effectiveness and, ultimately, mission success. Collectively, these steps have become integral to developing Airmen into a ready cyber force capable of operating in joint and coalition environments.

By 2020, the Marine Corps will have deployable, full-spectrum cyberspace operations capabilities integrated into the MAGTF, enabling it to fight a single-battle across all five domains of warfare using a combined-arms construct. Three of thirteen MARFORCYBER CMF teams have achieved full operational capability and are operating in support of Marine Corps, USCYBERCOM, and combatant commander missions. As it enters the final stages of its CMF team build, MARFORCYBER is establishing the Marine Corps Cyber Warfare Group, which will be responsible for

manning, training, and equipping the Marine Corps CMF teams. To support the training and exercises of cyber units, MARFORCYBER is also developing a persistent training environment to enhance military occupational skills proficiency, test and develop next generation solutions, host remote training and education of Marine Corps operating forces, and refine tactics, techniques, and procedures.

JFHQ-DODIN has built capability through the workforce that it continues to assemble and through lessons learned from the frontlines of DODIN cyber activity. Before the creation of this operational headquarters, a Service responding to an attack on its network would deal with the problem more or less decisively, but in isolation, thus leaving other Services and agencies potentially vulnerable to the same attack. Information regarding the attack might be shared with other interagency partners, but there was no joint mechanism to alert the rest of the vast force of DOD network operators to a new threat. JFHQ-DODIN assumed this synchronizing responsibility.

People are the ultimate enabler of the joint cyber force, but they require tools and capabilities. The Service cyber components are building new capabilities for use in cyberspace, and sharing these with the joint force. One of the most critical components to maintaining our military's warfighting advantage is the ability to develop and rapidly field innovative cyber capabilities. The Air Force has established seven cyber weapons systems to ensure the cyber capabilities being presented to the joint community are properly organized, trained, and equipped to meet the demands of an increasingly contested domain. The Air Force Life Cycle Management Center has strived to streamline the ability to provide solutions to support cyber missions through its "Rapid Cyber Acquisition" and "Real Time Operations and Innovation" initiatives. These efforts have resulted in the fielding of capabilities that have thwarted adversary exploitation of user authentication certificates and the unauthorized release of personally identifiable information, while also helping to block sophisticated intrusion attempts. Many of these cyber solutions were developed and fielded in weeks or months and we need faster results.

ARCYBER is pursuing cyber analytics capabilities to gather unprecedented quantities of data across cyberspace, providing a clearer picture of Army networks, systems, and data. Coupled with architecture modernization, this effort is critical to protect the future force and its ability to fight and win. The director of DISA, who is dual-hatted as the commander of JFHQ-DODIN, hopes to leverage technology to improve operations and influence traditional warfighting concepts such as deception, maneuver, battlespace, passage of lines, and defense-in-depth to improve the overall defensive posture of the DODIN. One example is Software Defined Networks, which can provide the ability to create a network, and when necessary, kill a network and move the warfighters and assets to another network in a virtualized space, thus remaining resilient and agile in the protection and defense of our systems while ensuring the mission continues unhindered.

In the Fight Now

In cyberspace we are already in real or imminent contact with adversaries. Every day, opponents attempt to access the DODIN to establish persistent presences in the critical networks we rely on for mission success. The level of adversary activity varies greatly and is influenced by multiple factors, including geopolitical events and even significant anniversaries. DOD systems mitigate an average of two million "intrusion attempts" each month, not counting the billions of malicious emails that DOD receives annually, 85 percent of which are blocked by a filter or defensive capability.

Lieutenant General Alan Lynn, USA, commander of JFHQ-DODIN and director of DISA, highlighted the pace of operations for JFHQ-DODIN last fall: "[JFHQ-DODIN recently] stood up, so you would think we are just building it as we are flying it—and it would be kind of a slow process." But such a thought would be mistaken, General Lynn explained. JFHQ-DODIN had no time to grow and learn before being thrown into the fight: "We are absolutely in the fight now." The general cited seven named cyber operations that JFHQ-DODIN has been involved in since reaching initial operational capability in early 2015. Some were deployed operations, while others were launched from the component's Fort Meade headquarters. The first operation began only days after JFHQ-DODIN's inception, and required a deployed CPT to locate and mitigate the threat.

We can expect that pace to intensify in the years ahead. The JFHQ-DODIN experience typifies the pace of cyberspace operations for all USCYBERCOM components. Our current cyber quandary is not some passing phase—it is the new normal for the joint force. Indeed, it is the new normal for every government and military around the world. That is why USCYBERCOM published its vision last year. We have an opportunity to use our experience, our technology, and the investments we have already made in training and infrastructure to stay ahead of would-be adversaries that have arrived in cyberspace comparatively recently. We must also ensure that our ability to generate assured command and control continues even in a degraded environment—even as we also focus on developing mission capabilities to provide the joint force with more options within the cyber arena. USCYBERCOM, looking Beyond the Build, has a vision to do just that. **JFQ**