A HOOVER INSTITUTION ESSAY

US Cyber Command's First Decade

MICHAEL WARNER

Aegis Series Paper No. 2008

National Security, Technology, and Law

United States Cyber Command (USCYBERCOM) turned ten years old in 2020. It is a unique institution—a military command that operates globally in real time against determined and capable adversaries and yet never fires a shot or launches a missile. The Command comprises an amalgam of military, intelligence, and information technology capabilities that came together into its present shape more by design than by fortuitous chance. That design, however, was itself a work in progress.

The Command's first decade built upon the notion that states must operate in cyberspace at scale and in real time. "Operating" means that key national systems and data have to be "fought" like a weapons platform; in other words, they enable and execute critical sovereign functions and thus cannot be switched off or managed as discrete and individual devices.[1] Indeed, each system and device affects the whole, and that whole is now immense. Only operational processes can harness the military's and the government's limited talent and resources in ways that can accomplish such global tasks on behalf of the nation, and only military components have the training, expertise, equipment, and resources to fulfill key elements of that requirement full-time and without interruption.

That vision dawned on military and civilian leaders years before the establishment of USCYBERCOM. The Command then refined the vision through actual operations. USCYBERCOM was by no means a passive medium upon which other government and industry actors imposed their visions. On the contrary, the Command's leaders, experts, and experiences influenced the course of discussions and resulting decisions. The evolution began two decades back, as key decisions were made that framed the institutional context for USCYBERCOM. This history is interesting not only for what it says about military innovation and bureaucratic change in the US government, but also for the insight it offers on the development of other military cyber components among America's allies, partners, and adversaries.

Antecedents

The Joint Chiefs of Staff in 2004 labeled cyberspace a "domain" of military operations, meaning that the systems that processed, stored, and moved data in digital forms had collectively become a venue where states could use force to coerce other states. Thus that year's *National Military Strategy* declared that:

> [the nation's armed forces] must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace. Armed Forces must employ military capabilities to ensure access to these domains to protect the Nation, forces in the field and US global interests.[2]

This recognition of cyberspace as an arena for inter-state conflict and coercion might appear from the perspective of 2021 to be rather premature. Yet in 2004 it culminated almost two decades of public and private debates over the characteristics and prospects of cyberspace for national security.

Cyber capabilities began growing in America's intelligence agencies, armed services, and computer and telecommunications industries in the 1970s. For reasons beyond the scope of this essay, no single government actor possessed the situational awareness and authority to demand that users connecting to digital networks around the nation employ best practices (like patching, passwords, encryption, and enterprise management) that were well known—if haphazardly applied—in the computer security community.[3] Governmental and private capabilities through the 1980s evolved on relatively closed networks based on a variety of digital protocols. Technological and strategic events in the 1990s, however, created the modern security problem. Now-familiar debates over cybersecurity began in earnest with the global adoption of TCP/IP packet switching to link thousands of "intra-nets," as well as with the nearly simultaneous opening of dictatorial regimes to the internet in the mid-1990s.[4]

American experts soon grasped that other nations too could now employ what the RAND Corporation called "strategic information warfare" against the United States. A tabletop exercise at RAND in 1995 showed that America, with its "complex, interconnected network control systems for such necessities as oil and gas pipelines, electric grids, etc.," had become vulnerable even to states with much inferior militaries that were nonetheless willing to utilize cyber techniques to leapfrog US forces and hit America's critical infrastructure.[5] "In sum," RAND's report concluded, "the US homeland may no longer provide a sanctuary from outside attack."[6]

Even the Department of Defense (DoD) rapidly came to depend on globally networked digital infrastructure to run its routine business operations. Such networks could be largely hardware agnostic as long as they ran operating systems that could send emails and display pages on the new World Wide Web; thus the Department suddenly needed fewer costly and personnel-intensive DoD-tailored communications systems.[7] Yet linking military systems on digital infrastructures that were not only outside of DoD control but also used by millions of foreign (and essentially anonymous) actors also created an unprecedented "tunnel of vulnerability" for the nation, as the DoD Defense Science Board warned in 1996.[8] Congressional auditors that same year recorded their concern with these developments, noting that "major disruptions to military operations and readiness could threaten national security if attackers successfully corrupted sensitive information and systems or denied service from vital communications backbones or power systems."[9] Such concerns heightened in 1998, when DoD network administrators spotted a set of intrusions into US government systems that American observers soon dubbed "Moonlight Maze."[10] Michael Vatis of the Federal Bureau of Investigation (FBI) put these developments in context for Congress in 1999:

> In the past few years we have seen a series of intrusions into numerous Department of Defense computer networks as well as networks of other federal agencies, universities, and private sector entities. Intruders have successfully accessed US Government networks and took large amounts of unclassified but sensitive information. . . . It is important that the Congress and the American public understand the very real threat that we are facing in the cyber realm, not just in the future, but now.[11]

The Information Revolution thereafter accelerated, locking in technological consequences almost before policy makers realized their significance. Military doctrine struggled to keep pace. Despite the fact that the Department of Defense had secretly foretold the rise of "information warfare" as early as 1992, the Joint Chiefs of Staff in 1996 decided that offensive and defensive cyber operations should be treated doctrinally as facets of "information operations."[12] This temporarily grouped the rapidly evolving and highly specialized skill sets for defending and attacking digital data and networks with a set of tangentially related missions such as psychological warfare, electronic warfare, and operations security.[13]

The Department of Defense soon developed an operational approach to securing its information systems. It created an organization in 1998 to guide such efforts —the Joint Task Force–Computer Network Defense (JTF-CND)—and tapped experts at the National Security Agency (NSA) to help identify threats to its networks. The Clinton Administration's subsequent national cybersecurity strategy hinted that the Agency's contribution stemmed in part from its intelligence capabilities: "The NSA is uniquely qualified to serve its customers/partners because of its ability to perform in-depth technical analysis of serious intrusions and because it is the only organization positioned to link intrusion data to foreign signals intelligence."[14] JTF-CND helped invent and apply the concept of "NetOps" for sustaining the capabilities of DoD's Global Information Grid (GIG), which itself had become indispensable for the US military's operations. US Strategic Command (USSTRATCOM) would inherit JTF-CND's successor in 2002 and then refine and summarize NetOps as its operational construct for operating and defending the GIG:

> The goal of NetOps is to provide assured and timely net-centric services across strategic, operational and tactical boundaries in support of DOD's full spectrum of war fighting, intelligence and business missions. The desired effects of NetOps are: assured system and network availability, assured information protection and assured information delivery.[15]

In the early 2000s, a rough consensus developed in the Department of Defense that the United States must employ its military to operate in cyberspace at scale and in real time. Secretary of Defense Donald Rumsfeld explained this in his Information Operations Roadmap, published in classified form in October 2003 and released with redactions three years later. The DoD systems, and foreign threats to them, were growing so fast that they required a robust "defense in depth" based on the premise that "the Department will 'fight the net' as it would a weapons system."[16] Like ships at sea, DoD's networks had to sustain unbroken operations on a global scale despite the constant threat of degradation from adversarial action. Commanders therefore must be assured that system defenses would "ensure the graceful degradation of the network rather than its collapse."[17] The conclusion that Secretary Rumsfeld and the Department drew was that only operational processes could harness limited talent and resources in ways that could cope with such a global, real-time task, and only military components had the training, expertise, equipment, and resources to meet that DoD requirement.

That consensus resulted in Secretary Rumsfeld's creation of two joint military cyber components. The Clinton administration in 2000 had merged JTF-CND with the military's relative handful of computer-network-attack planners in a joint task force (the Joint Task Force–Computer Network Operations) under US Space Command. Secretary Rumsfeld two years later shifted that unit into the reorganized USSTRATCOM. In 2004 he split the unit into defensive and offensive components, respectively the Joint Task Force–Global Network Operations (JTF-GNO), and the Joint Functional Component Command–Network Warfare (JFCC-NW). The point of this institutional shuffle was to keep both elements under a functional combatant commander in USSTRATCOM while allowing them to grow to perform the tasks that confronted them. Both components would now be headed by three-star general officers, both of whom were "dual-hatted" as heads of combat support agencies (the Director of NSA [DIRNSA] for JFCC-NW, and the Director of the Defense Information Systems Agency [DISA] for JTF-GNO).

Modest operational successes for each joint task force helped convince Secretary of Defense Robert Gates in 2008 that they could and should be linked under a single commander. Hence, in June 2009, Secretary Gates directed USSTRATCOM "to establish a subordinate unified command designated as U.S. Cyber Command (USCYBERCOM)." JFCC-NW and JTF-GNO personnel would be reassigned to USCYBERCOM, which Gates "preferred" to see based at Fort Meade with NSA.[18]

The armed services at the same time began reorganizing their cyber capabilities, creating headquarters units (in addition to those already assigned to USSTRATCOM) to function alongside the emerging USCYBERCOM. These components (in 2010) were the Army Cyber Command; Marine Forces Cyber Command; Fleet Cyber Command/US Tenth Fleet; and Air Force Cyber Command/24th Air Force. USSTRATCOM delegated operational control of various Service cyber units (and their headquarters) to USCYBERCOM in late 2010.[19]

Creation and Early Steps

USCYBERCOM thus began operations in 2010 with the merger of JTF-GNO and JFCC-NW under the command of the officer who also directed NSA.[20] The Command has since performed three main missions: (1) defending the DoD information systems, (2) supporting joint force commanders with cyberspace operations, and (3) defending the nation from significant cyberattacks. The Command has worked at home and abroad to employ military capabilities at scale against adversaries in and through cyberspace, conducting most of its missions in collaboration with various partners, including the other Combatant Commands, federal agencies, intelligence services, allied forces, and industry experts.

The Command has worked under three commanders. Each officer gained his fourth star upon appointment to the post. Each also came to the job with significant professional experience in intelligence, and all three likewise served as the "dual-hatted" director of NSA. General Keith B. Alexander (US Army) advocated for the Command's creation and served as its first head from 2010 to 2014. Admiral Michael S. Rogers (US Navy) succeeded him and led USCYBERCOM as it grew from 2014 to 2018. General Paul M. Nakasone (US Army), the current commander, took over on May 4, 2018, the day USCYBERCOM was elevated to full unified Combatant Command status.

Several issues faced the new command at its inception. An internal analysis summarized them as "building capability and capacity in Service cyber forces, and gaining the requisite authorities and fully resourcing the Command."[21] Each of these issues in turn presented an interlocking series of complications. USCYBERCOM had to determine how it would exercise command and control over the Service cyber components that were assigned to it, and also had to plan how it would integrate its operations with those of the geographic combatant commands. The Command also started out with fewer people than it needed. Its combined JFCC-NW and JTF-GNO numbers totaled just over five hundred FY10 billets, versus the nine hundred–plus its headquarters had been projected to have in FY12 to perform its expanded missions.[22] In addition, in its haste to begin operations, USCYBERCOM sacrificed proficiency for speed. Admiral Rogers told Congress in 2015 that he had arrived at USCYBERCOM a year earlier and found it had been (for understandable reasons) sub-optimally constructed:

> The organizations had been well scoped and granted the authorities necessary to do our work. The bad news was that USCYBERCOM was built from the ground up by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to build mission capabilities as fast as possible.[23]

The Cyber Mission Force

As USCYBERCOM grew, leaders in the White House, Congress, and the Department of Defense responded to its requirements for additional resources and clarified authorities.

The Command created the Cyber Mission Force (CMF) in 2013 to orient the armed services in their task of manning, training, and equipping the nation's military cyberspace forces. The CMF was designed to overcome the problem of force presentation that plagued cyberspace operations from the outset.[24] The issues involved in this project were two. The first and most critical was a talent gap in the US military and across the nation. General Alexander explained this to Congress in early 2012:

> At present we are critically short of the skills and the skilled people we as a Command and a nation require to manage our networks and protect US interests in cyberspace. Our prosperity and our security now depend on a very skilled technical workforce, which is in high demand both in government and industry. We in DoD need to build a cyber workforce that can take action quickly across the full range of our mission sets as necessary. This will require us to adopt a single standard across the Department and the Services, so that we can truly operate as a single, joint force.[25]

Second, the available talent was not yet well allocated and organized, even with roughly eleven thousand people in the "force mix" across USCYBERCOM and its Service components. Each Service organized, trained, and equipped its "cyber" forces in various ways.[26] This made it difficult for anyone to understand just how much "combat power" DoD could dedicate to particular operations or concerns. "We need to foster a common approach to force development and force presentation—up to and including the Service component and joint headquarters—given the intrinsically joint nature of this domain," explained General Alexander to Congress in 2013.[27]

The Cyber Mission Force, Alexander assured Congress, would become a "high-quality, certified, and standardized force." It would increase predictability and decrease risk for joint force commanders receiving these increments of cyber power:

> We will be able to present cyber forces with known capability sets to our Combatant Commanders—forces they can train with, plan for, plan on, and employ like forces and units [in] any other military domain. This gets at the essence of normalizing cyber capabilities for the Department of Defense.[28]

Deputy Secretary of Defense Ashton Carter in late 2012 approved the creation of the CMF, setting the dimensions of the force at 133 teams and 6,187 billets—a manpower cost that one key Congressman publicly told General Alexander was "enormous."[29] Yet the Department and General Alexander held to the plan, telling Congress in 2014: "I am convinced we have found a force model that will give useful service as we continue to learn and improvise for years to come."[30]

CMF teams came in three types, each intended to represent a standard increment of combat power for cyberspace operations, as General Alexander explained to Congress in 2014:

> This force has three main aspects: (1) Cyber National Mission Teams to help defend the nation against a strategic cyberattack on our critical infrastructure and key resources; (2) Cyber Combat Mission Teams under the direction of the regional and functional Combatant Commanders to support their objectives; and (3) Cyber Protection Teams to help defend [the] DoD information environment and our key military cyber terrain.[31]

The 133 CMF teams would be built and presented by the armed services, with each service assigned a set number of teams to build and 42 work roles to fill.[32] Secretary of Defense Chuck Hagel reported to Congress that the types of teams were distributed as follows:

- 13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs)
- 27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs)
- 18 National Cyber Protection Teams (CPTs)
- 24 Service CPTs
- 26 Combatant Command and DoD Information Network CPTs[33]

Creating the teams took until 2016, and building them all to full operational capability subsequently took until mid-2018.

Standardization of team training and capability, as well as of organization, was a primary USCYBERCOM goal in building the CMF. Joint force commanders employing these teams, as well as other agencies and forces operating alongside them, needed to know that they could not only perform their missions, but could do so with minimal risk to friendly operations. General Alexander explained to Congress how this goal would be reached:

> The training for this force is happening now on two levels. At the team level, each cyber mission team must be trained to adhere to strict joint operating standards. This rigorous and deliberate training process is essential; it ensures the teams can be on-line without jeopardizing vital military, diplomatic, or intelligence interests. Such standards are also crucial to assuring intelligence oversight and to securing the trust of the American public that military operations in cyberspace do not infringe on the privacy and civil liberties of US persons. Our training system is in the midst of certifying thousands of our people to high and joint military-wide standards.
>
> At the individual level, we are using every element of capacity in our Service schools and in NSA to instruct members of the Cyber Mission Force teams.[34]

While building the CMF teams, USCYBERCOM added two operating components to employ its own NMTs and CPTs for specialized missions. The first of these, the Cyber National Mission Force (CNMF), came into being under the Commander of USCYBERCOM in early 2014; General Alexander called this "the US military's first joint tactical command with a dedicated mission focused on cyberspace operations."[35] The Joint Force Headquarters–DoD Information Networks (JFHQ-DoDIN) stood up a year later under the control of the second Commander of USCYBERCOM, Admiral Michael S. Rogers, who explained the new component to Congress in 2015:

> JFHQ-DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses. Placing the just-established JFHQ-DoDIN under USCYBERCOM gives us a direct lever for operating DoD's information systems in ways that make them easier to defend, and tougher for an adversary to affect. It also gets us closer to being able to manage risk on a system-wide basis across DoD, balancing warfighter needs for access to data and capabilities while maintaining the overall security of the enterprise.[36]

JFHQ-DoDIN brought operational perspectives and intelligence to bear on problems confronting local systems administrators and cybersecurity service providers (CSSPs), and was co-located with the Defense Information Systems Agency (DISA), whose three-star director also served as JFHQ-DoDIN's commander.

Shifting Strategic and Policy Contexts

Significant developments in cyberspace operational authorities and doctrine occurred in 2012. Late that year, President Obama approved Presidential Policy Directive 20 (PPD-20) to govern cyberspace operations outside of US networks. The directive—which remains classified but was publicly summarized by the White House—established "principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools." Its goal was "a whole-of-government approach consistent with the values that we promote domestically and internationally," and it sought that goal through "exercising restraint in dealing with the threats we face." PPD-20 sought to ensure that the US government took "the least action necessary to mitigate threats" and gave priority to "defense and law enforcement as preferred courses of action."[37]

The Obama administration that same year complained that adversaries who might be deterred from attacking the United States in cyberspace manifestly were not being deterred from trying to infiltrate US military, government, and critical infrastructure systems. Secretary of Defense Leon Panetta described their threatening behavior, warning that:

> We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity [*sic*] and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.[38]

A coordinated series of such attacks, warned Secretary Panetta, "could be a cyber Pearl Harbor" that worked to "paralyze and shock the nation."[39]

General Alexander recognized this peril, though he seemed optimistic that USCYBERCOM had attained a degree of offensive power that would enable the United States to retaliate for cyberattacks that caused physical destruction or loss of life. This deterrence-enhancing capability of the Command was rarely discussed in public, a fact that makes two such instances all the more noteworthy. Asked about the Command's combat power at a 2012 hearing, General Alexander explained:

> The co-location of Cyber Command with the National Security Agency provides our Command with "unique strengths and capabilities" for cyberspace operations planning and execution. I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up the Department's assertion that any actor contemplating a crippling cyberattack against the United States would be taking a grave risk.[40]

At another hearing a year later, General Alexander added:

> We believe our offense is the best in the world. Cyber offense requires a deep, persistent and pervasive presence on adversary networks in order to precisely deliver effects. We maintain that access, gain deep understanding of the adversary, and develop offensive capabilities through the advanced skills and tradecraft of our analysts, operators and developers. When authorized to deliver offensive cyber effects, our technological and operational superiority delivers unparalleled effects against our adversaries['] systems.[41]

While General Alexander professed his "confidence in our ability to deter major state-on-state attacks in cyberspace," he also worried that hostile reconnaissance like that described above by Secretary Panetta seemed to have no remedy. In short, USCYBERCOM had attained an ability to react, but it had not yet learned how to anticipate or prevent cyberattacks. As General Alexander publicly lamented in 2013, "we are not deterring the seemingly low-level harassment of private and public sites, property, and data."[42]

By Admiral Rogers's second year as commander, he and other leaders had concluded that adversaries held the ability to strike America's critical infrastructure in ways that neither the Command nor the nation could yet prevent. Admiral Rogers publicly explained this situation to Congress in September 2015:

> Digital tools in cyberspace give adversaries cheap and ready means of doing something that until recently only one or two states could afford to do: that is, to reach beyond the battle-field capabilities of the US military. They have demonstrated the capacity to hold "at risk" our military and even civilian infrastructure. . . . We have recently seen Russian- and Chinese-sponsored intrusions in United States information systems—penetrations that were designed to (and in some cases did) gain persistent presence in the targeted networks.[43]

Senate Armed Services Committee chair John McCain (R-AZ) at that same hearing complained that adversary actions in cyberspace ventured well beyond harassment. He blamed the Obama administration for this state of affairs, expressing his unhappiness about its approach to cyber operations policy and strategy:

> Make no mistake, we are not winning the fight in cyberspace. Our adversaries view our response to malicious cyberactivity as timid and ineffectual. Put simply, the problem is a lack of deterrence. As Admiral Rogers has previously testified, the administration has not demonstrated to our adversaries that the consequences of continued cyberattacks against us outweigh the benefit. Until this happens, the attacks will continue, and our national security interests will suffer. . . . Establishing of cyberdeterrence also requires robust capabilities, both offensive and defensive, that can pose a credible threat to our adversaries.[44]

Senator McCain was no outlier in his call for better deterrence. Admiral Rogers hinted in spring 2016 that change was needed because cyber actors could now affect security conditions at a national level; i.e., they could cause strategic effects: "Some of these threat actors are seeking to shape us, narrowing our options in international affairs to limit our choices in the event of a crisis."[45] Although a deterrence posture had not stopped such effects and seemed unable to mitigate them, Senator McCain and Admiral Rogers nonetheless saw the solution in more and better deterrence. Indeed, deterrence had been the strategic frame for DoD since the Cold War. The Joint Chiefs of Staff had almost by default classed cyberspace operations in that frame, as can be seen in this passage from the 2004 edition of the *National Military Strategy*:

> The non-linear nature of the current security environment requires multi-layered active and passive measures to counter numerous diverse conventional and asymmetric threats. These include . . . threats in cyberspace aimed at networks and data critical to US information-enabled systems. *Such threats require a comprehensive concept of deterrence encompassing traditional adversaries, terrorist networks and rogue states able to employ any range of capabilities.*[46]

Despite the dominance of deterrence thinking, however, Admiral Rogers also hinted to Congress in 2016 that a reconsideration of that paradigm had begun. He explained:

> We at USCYBERCOM are thinking more strategically about shifting our response planning from fighting a war to also providing decision makers with options to deter and forestall a conflict before it begins. These new options would be in addition to capabilities that help our combatant commanders succeed in their missions if and when conflict erupts and the joint forces receive an "execute order" to commence kinetic as well as cyberspace operations.[47]

As this rethinking progressed, the Obama administration launched a related debate over the wisdom of elevating USCYBERCOM from a sub-unified to a full unified combatant command. Discussions had commenced in 2012 but became public knowledge in early 2016, with Admiral Rogers feeling confident enough in its likelihood to advocate elevation while testifying before the sympathetic Chairman McCain. At the same time, however, sentiment arose in the administration in favor of splitting the "dual-hat" command relationship between USCYBERCOM and NSA. Admiral Rogers felt USCYBERCOM was unready for such a split, even if it came with elevation to unified command status.[48] Senator McCain agreed, and publicly scolded the administration that September after hearing rumors that the "dual-hat" would end soon:

> I'm troubled by recent reports that the Obama administration may be trying to prematurely break the dual-hat before . . . President Obama leaves office. [Four days earlier] it was reported that Secretary of Defense Ash Carter and Director of National Intelligence James Clapper have backed a plan to separate Cyber Command and the NSA. . . . I do not believe rushing to separate the dual-hat in the final months of an administration is appropriate, given the very serious challenges we face in cyberspace and the failure of this administration to develop an effective deterrence policy.[49]

Subsequent reporting suggested that Senator McCain's concern was not misplaced. The *Washington Post* noted anonymous tips indicating that Secretary Carter and Director of National Intelligence James Clapper had "recommended to President Obama that the director of the National Security Agency, Adm. Michael S. Rogers, be removed."[50] The firing had not occurred, alleged the *Post*'s Ellen Nakashima, because it was "tied to another controversial recommendation: to create separate chains of command at the NSA and the military's cyberwarfare unit, a recommendation by Clapper and Carter that has been stalled because of other issues."[51] President Obama declined to act on their recommendation in his final weeks in office. Asked about the rumor while attending a conference in Peru, the president publicly called Admiral Rogers "a terrific patriot [who] has served this country well in a number of positions."[52] Yet President Obama insisted that a split of the dual-hat was indicated:

> After directing a comprehensive review of this issue earlier this year, and consistent with the views of the Secretary of Defense and the Director of National Intelligence, I strongly support elevating CYBERCOM to a unified combatant command and ending the dual-hat arrangement for NSA and CYBERCOM. . . . The two organizations should have separate leaders who are able to devote themselves to each organization's respective mission and responsibilities, but should continue to leverage the shared capabilities and synergies developed under the dual-hat arrangement.[53]

Operating in Cyberspace

Incoming president Donald Trump retained Admiral Rogers for over a year and asked the new secretary of defense, James Mattis, to make recommendations regarding elevation and the dual-hat issue. Congress influenced the Secretary's deliberations, having added (in the same National Defense Authorization Act for FY17) a provision in 10 USC. § 167b directing the Executive Branch to create "a unified combatant command for cyber operations forces."[54] Secretary Mattis thus decided to elevate the Command under Rogers's successor, who ultimately proved to be the US Army's Paul M. Nakasone. The succession occurred on May 4, 2018, the same day that US Cyber Command became a unified combatant command (when Nakasone, now general, pinned on his fourth star). Secretary Mattis made no decision on the dual-hat, and thus General Nakasone served as both Commander, USCYBERCOM, and Director, NSA.

USCYBERCOM during this time engaged adversaries in a variety of offensive and defensive operations. For a sense of how its engagement evolved, it helps to glance at General Alexander's valedictory Congressional testimony in 2014, in which he summarized developments and offered members a glimpse of the future shortly before retiring. His remarks were important as much for what he implied as for what he mentioned. Looking back over the previous decade, General Alexander noted:

> The level and variety of challenges to our nation's security in cyberspace differs somewhat from what we saw and expected when I arrived at Fort Meade [as Director, NSA] in 2005. At that time many people, in my opinion, regarded cyber operations as the virtual equivalents of either nuclear exchanges or commando raids. What we did not wholly envision were the sort of cyber campaigns we have seen in recent years. Intruders today seek persistent presences on military, government, and private networks (for the purposes of exploitation and disruption). These intruders have to be located, blocked, and extracted over days, weeks, or even months. Our notion of cyber forces in 2005 did not expect this continuous, persistent engagement, and we have since learned the extent of the resources required to wage such campaigns, the planning and intelligence that are essential to their success, and the degree of collaboration and synchronization required across the government and with our allies and international partners.[55]

There is a lot to unpack in this statement. Essentially it showed USCYBERCOM in 2014 pondering its need to operate at different strategic, operational, and tactical levels in the United States and abroad, and with varying degrees of freedom to maneuver in each.

Within Department of Defense systems in the United States and abroad, USCYBERCOM operated to defend the US military in cyberspace—a mission at least as important as its offensive mission. USCYBERCOM performed its defensive missions until 2018 under USSTRATCOM's Operation Gladiator Phoenix, which Secretary Gates had endorsed in early 2011.[56] While defenses improved, the "attack surface" provided by DoD's millions of network devices proved a tempting target that was too large to defend at all points. In 2013, for instance, cyber actors found a breach in the Navy Marine Corps Intranet (NMCI), a huge system that Congressional staffers called "an unclassified but important and pervasive internal communications network."[57] Senator McCain asked then vice admiral Rogers at his confirmation hearing about the intrusion, which Rogers agreed was indeed a significant penetration:

> As a result, I directed a rather comprehensive operational response to that. That response was much broader than just be able to come back and say they're not there anymore. I wanted to use this as an opportunity to try to drive change. So we put a much more comprehensive, much longer term effort in place.[58]

Vice Admiral Rogers implied that traditional distinctions between operational and "business" systems had grown obsolete.[59] All systems had to be defended, because a penetration of even an unclassified network could cause significant disruption for the US military. Rogers's successor at Tenth Fleet (and the first woman to command a numbered fleet), Vice Admiral Jan Tighe, sketched the new dynamic in 2014:

> To some extent, the new cyber norm is a big challenge—every day we're under some type of threat. Fighting our networks every day and making sure we're providing for and operating networks that are secure is job one. That's looking at both the threats that are coming after us and the vulnerabilities that are inherent and always going to be there—and what we do to lower that risk calculus for the entire Navy, and share that knowledge and information with our other services and components to ensure the whole DoD is better.[60]

The Navy and (by implication) the larger military was undergoing a "cultural shift" toward recognizing this challenge, Vice Admiral Tighe explained, but while Navy leaders grasped the problem, not everyone shared this awareness. Indeed, "as you get lower down the food chain, it gets a lot more spotty—there are pockets of understanding, there are pockets of non-understanding."[61]

USCYBERCOM's offensive operations initially concentrated on terrorist targets—making them like the "commando raids" that General Alexander alluded to above. These missions increased in complexity and tempo as a result of Secretary of Defense Ashton Carter's decision to employ them in support of the overall coalition campaign (Operation Inherent Resolve) against the Islamic State in Iraq and Syria (ISIS). Admiral Rogers created a dedicated element for this fight in mid-2016, establishing Joint Task Force ARES under Army Cyber Command. As these efforts developed, senior officials grew less reticent in describing them to the public; Deputy Secretary of Defense Robert Work told reporters in April 2016 the US military was dropping "cyber bombs" on ISIS.[62]

The cyberspace campaign against ISIS received mixed reviews. Secretary of Defense Ashton Carter discounted it: "I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques."[63] This was not wholly the fault of USCYBERCOM, Carter added. When the Command did produce "something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection"; thus "none of our agencies showed very well in the cyber fight." Secretary Carter's criticism may reflect his temporal vantage point; he left office in January 2017, just as the ground offensive against ISIS accelerated and supporting cyber effects increased. General Joseph L. Votel, commander of US Central Command, praised the conduct of cyberspace operations in support of his forces:

> At the tactical level, we have integrated [cyberspace operations] and fielded cyberspace capabilities to support Special Forces and, more recently, conventional ground forces. These tactical cyberspace and [electronic warfare] capabilities are synchronized with the ground scheme of maneuver providing an additional level of force protection to the warfighter by disrupting the adversaries' ability to command and control their forces in the battlespace.[64]

Then lieutenant general Stephen Townsend, who commanded Operation Inherent Resolve (2016–17), publicly noted a synergy between conventional and cyber missions for more than force protection. A reporter summarized one of General Townsend's examples of cyberspace operations enabling kinetic strikes:

> The coalition identified primary command posts ISIS was operating from but didn't know where alternate command posts were located. Rather than hitting the sites with missiles and having the militants be unknown for a while, Townsend said, they used "multidomain operations capabilities" from space and cyber to deny the enemy's primary command posts, forcing them to move and unveil alternate command posts. Once identified, the coalition struck the alternate command posts, working its way back to the primary sites. . . . While the operation overall was a success, Townsend said it took weeks to plan with only about a week of payoff.[65]

Both Secretary Carter and General Votel also hinted at cyberspace successes against ISIS propaganda and media outlets. One bright spot for cyberspace operations, Carter noted, was the "international effort to combat ISIS's hateful online presence with countermessaging, an effort that did achieve significant reach and had a real impact."[66] General Votel added that "our first success at true multidomain operations through synchronized lethal and nonlethal effects was against ISIS's critical media operatives; we denied key infrastructure and degraded their ability to execute external operations through social media."[67] Newly declassified documents offer some details on this campaign.

The most prominent and consequential operation against ISIS media efforts was code-named Operation Glowing Symphony (OGS) and began in late 2016. Occasional "commando raid" missions against ISIS had been episodic and lacked impact, noted National Public Radio reporter Dina Temple-Raston (in an article for which she was allowed to interview USCYBERCOM leaders and OGS participants):

> U.S. Cyber Command had been mounting computer network attacks against the group, but almost as soon as a server would go down, communications hubs would reappear. The ISIS target was always moving and the group had good operational security. Just physically taking down the ISIS servers wasn't going to be enough. There needed to be a psychological component to any operation against the group as well.[68]

Only a tightly synchronized campaign against ISIS media operations would work, but fortunately USCYBERCOM learned the group ran its media empire through a handful of accounts and servers. This was careless; ISIS network administrators had taken "a shortcut and kept going back to the same accounts to manage the whole ISIS media network. They bought things online through those nodes; they uploaded ISIS media; they made financial transactions. They even had file sharing through them."[69]

The complication for USCYBERCOM emerged from the globally distributed nature of those ISIS media nodes. The Command had authorization to support Operation Inherent Resolve where US forces were directly engaged in Iraq and Syria, but striking targets outside of this "area of responsibility" required extensive interagency coordination and White House approval. "The amount of informal meetings, briefings, and overall information sharing that occurred was extremely in-depth and time consuming for both USCYBERCOM and JTF ARES staffs," complained a USCYBERCOM after-action review.[70] Indeed, noted a briefing prepared in USCYBERCOM a couple weeks into OGS, interagency coordination was so cumbersome because "deconfliction processes were too immature to execute operational deconfliction."[71] One reporter summarized documents recently released by the Command under Freedom of Information Act requests as follows, quoting internal USCYBERCOM complaints:

> "Interagency policies and processes are not established to meet the demand for speed, scale, and scope required for effective cyberspace operations," the documents say. . . . In one case, deliberations in the National Security Council Principals Committee . . . took so long that

> they delayed some Glowing Symphony missions, possibly to the detriment of the operation's goals. "The time required to elevate and negotiate the Interagency non-concurs prevented USCYBERCOM from [redacted] as originally designed," one briefing document says.[72]

Nevertheless, OGS eventually won approval in the interagency review process and launched synchronized strikes against the key ISIS media nodes on a single night in November 2016, according to Temple-Raston's account for NPR:

> Once they had taken control of the 10 nodes, and had locked key people out of their accounts, ARES operators just kept chewing their way through the target list. "We spent the next five or six hours just shooting fish in a barrel," [a USCYBERCOM operator] said. "We'd been waiting a long time to do that and we had seen a lot of bad things happen and we were happy to see them go away."[73]

General Nakasone, who commanded JTF-ARES that night, told Temple-Raston that the early results from OGS were impressive:

> Within the first 60 minutes of go, I knew we were having success. . . . We would see the targets start to come down. It's hard to describe but you can just sense it from being in the atmosphere, that the operators, they know they're doing really well. They're not saying that, but you're there and you know it.[74]

Over the next several months, OGS operators (with help from coalition partners) harassed the ISIS media outlets.[75] ISIS's online presence never vanished, of course, but such an unrealistic goal was never proposed as an objective of Glowing Symphony. OGS should be appraised for its contribution to Operation Inherent Resolve's overall goal of eradicating ISIS's territorial base and hampering its global reach. General Nakasone told Congress in early 2020 that ISIS had lost the initiative online:

> ISIS is now mostly confined to publishing text-only products, instead of their previous, gruesome multi-media products. These products used to be disseminated in multiple languages through mass-market platforms. Now, ISIS struggles to publish in non-Arabic languages and is confined to less-traditional messaging applications. Of course, the collapse of the physical caliphate made it harder for ISIS to operate online. But Cyber Command's efforts through JTF-ARES remain important to contesting ISIS's attempts at establishing a virtual caliphate as well.[76]

A USCYBERCOM after-action review called Glowing Symphony "the most complex offensive cyberspace operation that USCYBERCOM has undertaken to date."[77] The reviewers hinted that the operation would have lasting effects on the conduct of offensive cyberspace operations: "The scale and complexity of OGS has also allowed us to learn a number of lessons that will benefit the community as we move forward."[78] General Votel seemed to agree on the utility of lessons gained from the overall campaign in cyberspace: “These operations against ISIS have informed efforts across CENTCOM as well as other Combatant Commands.”[79]

A New Operational Paradigm

Executive and legislative guidance in 2018 expanded the scope of military cyberspace activities in operations short of armed conflict. Congress affirmed that August via the National Defense Authorization Act for Fiscal Year 2019 that clandestine military operations against adversary activities in cyberspace could proceed as “traditional military activity” under the exceptions provided for in the covert action statute.[80] The same act encouraged “active defense” in cyberspace against Russia, China, North Korea, and Iran. This provision offered the president the authority to order US Cyber Command “to disrupt, defeat, and deter cyberattacks” by nations that conduct an “active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes.”[81] President Trump implemented these provisions in part through National Security Presidential Memorandum 13 (NSPM-13), the still-classified guidance that rescinded the procedures mandated by PPD-20.[82]

Cyber operations undertaken below the level of armed conflict would now be guided by the concept of “persistent engagement.” USCYBERCOM proposed this in a public white paper that Admiral Rogers approved in March 2018. This Vision Statement, as it soon became known, summarized the rationale and thrust of the concept as follows:

> Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks. We will pursue attackers across networks and systems to render most malicious cyber and cyber-enabled activity inconsequential while achieving greater freedom of maneuver to counter and contest dangerous adversary activity before it impairs our national power.[83]

Rogers’s successor, General Nakasone, endorsed persistent engagement soon after taking command.[84] The Department of Defense in turn adopted and adapted it in the new *DoD Cyber Strategy* in September 2018, which applied the term “Defend Forward” to describe the overall strategy, within which persistent engagement would now be considered the operational approach. The secretary’s principal cyber advisor, Kenneth Rapuano, explained this to Congress in early 2020:

> The Department defends forward by conducting operations that range from collecting information about hostile cyber actors, to exposing malicious cyber activities and associated infrastructure publicly, to directly disrupting malicious cyber actors. In

> order to be successful, we must be in malicious cyber actors' networks and systems and continually refresh our accesses, capabilities, and intelligence. Defending forward simultaneously puts "sand in the gears" of the offensive operations of malicious cyber actors, and generates the insights that enable our interagency, industry, and international partners to strengthen their resilience, address vulnerabilities, and defend critical networks and systems.[85]

By the time Assistant Secretary Rapuano testified, the department and USCYBERCOM could cite a recent application of the "Defend Forward" strategy. The 2016 US presidential race had been famously targeted by Russian cyber actors, who worked to sow division in the American electorate.[86] Their efforts corresponded with leaks of emails exfiltrated by Russian intelligence from the headquarters of the Democratic Party and released to the news media to embarrass Hillary Clinton's campaign.[87] To avoid a repeat of foreign interference with American democratic processes, the Trump administration two years later ordered the Department of Defense to assist the Department of Homeland Security (DHS) and the FBI in defending the upcoming midterm elections. National Security Advisor John Bolton revealed a week before the elections that the United States was conducting "offensive cyber operations" for this purpose; he had earlier explained, "Our hands are not tied as they were in the Obama administration."[88]

In this context, General Nakasone organized a "Russia Small Group" (RSG) to coordinate actions by USCYBERCOM and NSA in defense of the 2018 balloting. Together with interagency partners in DHS and the FBI, as he explained to Congress afterward, the RSG's effort "helped disrupt plans to undermine our elections." According to Nakasone:

> [USCYBERCOM in particular] executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.[89]

Gauging the success of the RSG is difficult without access to Russian records, but American observers regarded the lack of significant foreign interference in the midterms as a positive sign. "US officials believe the [American] disruption effort," observed columnist David Ignatius in the *Washington Post*, "has frazzled some of the Russian targets and may have deterred some interference during the midterms."[90] After hearing classified briefs on the operation, Senator Mike Rounds (R-SD) in early 2019 publicly asked General Nakasone if it would be fair to say that it was "not a coincidence that this election went off without a hitch." The general replied simply that "the security of the midterm election was the number one priority" at USCYBERCOM and NSA. Senator Richard Blumenthal (D-CT) rhetorically pressed this point, wishing that such operations could be more widely discussed: "Without going into any of the details, there are some successes that the American people should know happen[ed]."[91]

One particular RSG innovation, the "hunt forward" mission, continued after 2018. General Nakasone explained to Congress in early 2020 that USCYBERCOM's RSG element had deployed experts to search for intrusions on foreign governments' information systems:

> During multiple hunt forward missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.[92]

Assistant Secretary Rapuano added in the same hearing that CNMF's subsequent hunt-forward missions and malware releases (on the VirusTotal cybersecurity website) had allowed "organizations and individuals around the world to mitigate identified vulnerabilities, thereby degrading the efficacy of malicious tools and campaigns."[93] General Nakasone summarized the value of this effort later in 2020: "The net effect of the many hunt-forward missions that Cyber Command has conducted in recent years has been the mass inoculation of millions of systems, which has reduced the future effectiveness of the exposed malware and our adversaries."[94]

USCYBERCOM's faster operational tempo after 2016 produced a spiraling set of lessons regarding the intelligence, capabilities, personnel, and partners required for success in both defensive and offensive cyber operations. General Nakasone told NPR's Dina Temple-Raston that the experience gained by JTF-ARES in operating against ISIS influenced the direction of the Russia Small Group: "It provided us with a very, very good road map of what they might do in the future."[95] Lessons learned by the RSG, in turn, influenced the composition and tasking of a successor task force at USCYBERCOM and NSA, the Election Security Group (ESG), as General Nakasone explained to Congress in March 2020. "Last year," he noted, "we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond."[96] Partnerships and "persistent engagement with our adversaries," he predicted, would facilitate the ESG's work, "ensuring that exquisite intelligence drives tailored operations, which in turn generate more insight and opportunities to harden defenses and impose costs if necessary."[97] On Election Day 2020, General Nakasone gave a brief interview at which he spoke of a measure of success in the fact that the balloting saw no significant foreign disruption. He said he was "very confident in the actions that have been taken against adversaries over the last several weeks and several months to ensure they are not going to interfere in our elections."[98]

General Nakasone had suggested to Temple-Raston a few months earlier that USCYBERCOM had fulfilled its promise by attaining proficiency and permanence: "I think it's important for the American public to understand that as with any domain—air, land, sea, or space—cyberspace is the same way; our nation has a force."[99]

Conclusion

> When Cyber Command was established in 2010, the operative assumption was that its focus should be on trying to prevent the military's networks from being infiltrated or disabled. But a reactive and defensive posture proved inadequate to manage evolving threats. Even as the military learned to better protect its networks, adversaries' attacks became more frequent, sophisticated, and severe. We learned that we cannot afford to wait for cyberattacks to affect our military networks. We learned that defending our military networks requires executing operations outside our military networks. The threat evolved, and we evolved to meet it.[100]

US Cyber Command has instantiated an idea that emerged and developed over four successive presidential administrations and roughly ten congresses. Simply put, that notion holds that advanced states must operate in cyberspace at scale and in real time—which means they must use military entities to fill key national requirements. Various threats envisioned when USCYBERCOM began operations in 2010 have since come to pass: command elements now work every day against determined and capable cyber actors seeking to penetrate Department of Defense information systems and disrupt key military and national functions.

USCYBERCOM's course was not inevitable, however, and the nation could have found other solutions to the dilemma of operating in cyberspace. The Command at the time of this writing has a budget of $596 million (for FY20) and 1,778 military and civilian personnel (plus contractors). At the start of 2020, the Command rostered 5,094 active duty service members and civilians in its Cyber Mission Force.[101] Such resources might have come together in very different ways; indeed, USCYBERCOM might not have existed all. If it had not been created, the US government could, and probably would, have improvised various work-arounds for defensive and offensive functions. But at what cost in time, losses, and risk?

In this context, it is disconcerting even to imagine how much less secure the United States would be without USCYBERCOM's defensive efforts. There is no reason to believe that the highly capable adversaries that confront America and its democratic partners today would have abandoned or even slackened their respective quests to develop dangerous cyberspace capabilities if the United States had unilaterally forsaken (or even substantially slowed) its building of military cyberspace elements after the middle of the 2000s. Indeed, had the United States done so, its strategic situation in 2020 would be grave. Even with current challenges, however, the federal government still retains control of its information systems and US commanders around the world can still control their forces. These capabilities can no longer be taken for granted. They owe their safety in no small part to the functioning of USCYBERCOM.

USCYBERCOM's offensive achievements, on the other hand, appear more modest. Here one can point to, as evidence of success, the strategic (if not yet permanent) defeat of ISIS and the seeming determination of adversaries to keep cyber conflict under the threshold of armed conflict. The idea that the Command has offensive power, moreover, probably has had some deterrent effect, supplementing the massive strength of America's nuclear and conventional forces. Finally, the Command's genesis and growth probably have also persuaded other actors to build their own military cyber forces. With that probability acknowledged, it seems safe to say that USCYBERCOM has kept the nation safer.

The Command's Cyber Mission Force played a key role in both its offensive and defensive achievements. It created teams that offered predictable increments of power in cyberspace, and mandated readiness and capabilities to bring the teams to a higher plane and make them more responsive and agile in their missions. Whether USCYBERCOM has influenced allies, partners, and adversaries to imitate it is a question that must be left for later scholars, but there has been no lack of foreign interest in the CMF model.

What does the future hold? USCYBERCOM will continue; there are no realistically foreseeable circumstances in which the US government decides it does not need to defend its military networks in a joint manner or to supplement DoD's combat operations with missions in cyberspace. On the contrary, USCYBERCOM could receive significant augmentations of resources and authorities, perhaps even midwifing the creation of a new military service, a "Cyberspace Force." Assuming these alternatives define the limits of the possible for USCYBERCOM, then it seems probable the Command will continue more or less on its present course for the next several years.

NOTES

[1] The definition of "operating" is broad and imprecise. As the Joint Chiefs of Staff explain:

> [The operational art is] a thought process to mitigate the ambiguity and uncertainty of a complex [operational environment] and develop insight into the problems at hand. Operational art also promotes unified action by enabling [joint force commanders] and staffs to consider the capabilities, actions, goals, priorities, and operating processes of interagency partners and other interorganizational participants, when they determine objectives, establish priorities, and assign tasks to subordinate forces. It facilitates the coordination, synchronization, and, where appropriate, the integration of military operations with activities of other participants, thereby promoting unity of effort.

Joint Chiefs of Staff, Joint Pub. 3-0, Joint Operations II-3 (2018).

[2] Joint Chiefs of Staff, The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow 18 (2004).

[3] I summarized these in Michael Warner, *Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003*, 37 IEEE Annals Hist. Computing 8 (2015). For an example of the sophistication that could be applied in the 1970s, see Staff of S. Comm. on Gov't Operations, 95th Cong., Computer Security in Federal Programs 135–38 (1977).

[4] Anthony Rutkowski, *Marking the 30th Anniversary of the Internet and Cybersecurity Treaty*, CircleID (June 22, 2020), http://www.circleid.com/posts/20200622-marking-30th-anniversary-of-the-internet-and-cybersecurity-treaty/.

[5] The exercise, based on a hypothetical clash with Iran, was described in Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, RAND, Strategic Information Warfare: A New Face of War xii, xvii (1996).

[6] *Id*.

[7] Albert J. Edmonds, C4I Issues, Presentation to the Program on Information Resources Policy, Center for Information Policy Research, Harvard University, in Guest Presentations, at 181–92 (1994); *see also* Albert J. Edmonds, Information Systems Support to DOD and Beyond, Presentation to the Program on Information Resources Policy, Center for Information Policy Research, Harvard University, in Guest Presentations, at 194 (1996).

[8] Office of the Undersec'y of Def. for Acquisition & Tech., Report of the Defense Science Board Task Force on Information Warfare-Defense, Exec. Summary (1996); *see also* Joint Chiefs of Staff, Joint Pub. 3-13.1, Joint Doctrine for Command and Control Warfare I-4 (1996).

[9] Gen. Acct. Off., Information Security: Computer Attacks at Department of Defense Pose Increasing Risks 4 (1996); *see also* Dan Verton, *IT Lessons Emerge from Kosovo*, FCW (Aug. 31, 1999), https://fcw.com/Articles/1999/08/31/IT-lessons-emerge-from-Kosovo.aspx.

[10] James Adams, *Virtual Defense*, 80 Foreign Aff. 98 (2001), https://www.foreignaffairs.com/articles/2001-05-01/virtual-defense.

[11] *Critical Information Infrastructure Protection: The Threat Is Real: Hearing before the S. Comm. on the Judiciary, Subcomm. on Tech. and Terrorism*, 106th Cong. 14 (1999) (statement of Michael A. Vatis, Fed. Bureau of Investigation).

[12] US Dep't of Def., DoD Directive No. TS 3600.1: Information Warfare (1992), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Administration_and_Management/14-F-0492_Directive_TS-3600-1.pdf?ver=2017-05-15-135850-923; US Dep't of Def., DoD Directive No. S-3600.1: Information Operations (1996), https://archive.org/stream/DODD_S3600.1/14F0492_DOC_02_Directive_S-3600.1_djvu.txt; *see also* Joint Chiefs of Staff, Joint Pub. 3-13.1, Joint Doctrine for Command and Control Warfare (1996).

[13] *See* Joint Chiefs of Staff, Joint Pub. 3-12, Cyberspace Operations (2018) (freeing offensive and defensive cyberspace missions from the doctrinal category of "information operations"). I discuss the evolution of relevant doctrine in Michael Warner, *Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014*, Cyber Def. Rev. (Aug. 27, 2015), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.

[14] Office of the President, Defending America's Cyberspace: National Plan for Information Systems Protection 41, 49 (2000).

[15] US Strategic Command, Joint Concept of Operations for Global Information Grid NetOps, iii (2005), https://www.hsdl.org/?abstract&did=685398; *see also* Bradley K. Ashley and Gary Jackson, *Information Assurance through Defense in Depth*, 3 IA Newsletter 3 (1999).

[16] US Dep't of Def., Information Operations Roadmap 44–49 (2003).

[17] *Id*.

[18] Memorandum from Robert M. Gates, Sec'y of Def., to Dep't of Def. Leadership, Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), https://fas.org/irp/doddir/dod/secdef-cyber.pdf.

[19] Michael Warner, *US Cyber Command's Road to Full Operational Capability, in* Stand Up and Fight! The Creation of US Security Organizations, 1942–2005, at 131 (Ty Seidule and Jacqueline E. Whitt eds., 2015).

[20] *Id*.

[21] *Id*.

[22] Keith B. Alexander*, Building a New Command in Cyberspace*, 5 Strategic Stud. Q. 3, 4, 10 (2011).

[23] *Department of Defense Authorization for Appropriations for Fiscal Year 2016 and the Future Years Defense Program: Hearing on S. 1376 before the S. Comm. on Armed Servs., Subcomm. on Intelligence, Emerging Threats and Capabilities*, 114th Cong. 415 (2015) [hereinafter 2015 Senate Hearings] (statement of Admiral Michael S. Rogers, Commander, US Cyber Command).

[24] In the American military system, the armed services raise, train, and equip forces, which they then "present" to the Combatant Commands that employ them in actual operations.

[25] *Department of Defense Authorization for Appropriations for Fiscal Year 2013 and the Future Years Defense Program: Hearing on S. 3254 before the S. Comm. on Armed Servs.*, 112th Cong. 971 (2012) [hereinafter 2012 Senate Hearings] (statement of Gen. Keith B. Alexander, Commander, US Cyber Command).

[26] *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force: Hearing before the H. Comm. on Armed Servs., Subcomm. on Intelligence, Emerging Threats and Capabilities*, 113th Cong. 63 (2013) [hereinafter 2013 House Hearings] (statement of Gen. Keith B. Alexander, Commander, US Cyber Command).

[27] *Id*. at 70.

[28] *Id*. at 71.

[29] *Department of Defense Authorization for Appropriations for Fiscal Year 2014 and the Future Years Defense Program: Hearing on S. 1197 before the S. Comm. on Armed Servs*., 113th Cong. 199–200 (2013) (statement of Gen. Keith B. Alexander, Commander, US Cyber Command); *see also* Office of Inspector Gen., US Dep't of Def., US Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams 2, 12–13 (2015). Rep. Jim Langevin commented: "I understand that Cyber Command [CYBERCOM] is beginning to organize itself into mission teams, which is an exciting step. But the manpower cost is enormous and the education and training requirement significant. This is going to take, obviously, a lot of work to get right." 2013 House Hearings, *supra* note 26, at 2.

[30] *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment: Hearing before the H. Comm. on Armed Servs., Subcomm. on Intelligence, Emerging Threats and Capabilities*, 113th Cong. 3 (2014) [hereinafter 2014 House Hearings] (written statement of Gen. Keith B. Alexander, Commander, US Cyber Command).

[31] *Id*. at 43–44.

[32] *See* 2013 House Hearings, *supra* note 26, at 85.

[33] US Dep't of Def., Quadrennial Defense Review 2014, at 41 (2014).

[34] 2014 House Hearings, *supra* note 30, at 5 (written statement of Gen. Alexander).

[35] *Id*.

36 2015 Senate Hearings, *supra* note 23, at 416 (statement of Admiral Rogers).

37 Office of the President, Fact Sheet on Presidential Policy Directive 20 (2013).

38 Secretary of Defense Leon Panetta, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), https://www.hsdl.org/?abstract&did=724128.

39 *Id*.

40 2012 Senate Hearings, *supra* note 25, at 8 (statement of Gen. Alexander).

41 *See* 2013 House Hearings, *supra* note 26, at 87.

42 *Id*. at 65.

43 *United States Cybersecurity Policy and Threats: Hearing before the S. Comm. on Armed Servs*., 114th Cong. 24–25 (2015) (statement of Admiral Michael S. Rogers, Commander, US Cyber Command).

44 *Id*. at 2 (statement of Sen. John McCain).

45 *Department of Defense Authorization for Appropriations for Fiscal Year 2017 and the Future Years Defense Program: Hearing on S. 2943 before the S. Comm. on Armed Servs*., 114th Cong. 462 (2016) [hereinafter 2016 Senate Hearings] (statement of Admiral Michael S. Rogers, Commander, US Cyber Command).

46 Joint Chiefs of Staff, *supra* note 2, at 18 (emphasis added).

47 2016 Senate Hearings, *supra* note 45, at 5 (statement of Admiral Rogers).

48 Jordana Mishory, *Rogers: CYBERCOM Should Be a Fully Unified Command, but Stay Dual-Hatted with NSA*, Inside Defense (Apr. 5, 2016), https://insidedefense.com/daily-news/rogers-cybercom-should-be-fully-unified-command-stay-dual-hatted-nsa; *see also* Jordana Mishory, *Lawmakers Want to Elevate CYBERCOM, Review Relationship with NSA*, Inside Defense (Apr. 25, 2016), https://insidedefense.com/daily-news/lawmakers-want-elevate-cybercom-review-relationship-nsa.

49 *Cybersecurity, Encryption and United States National Security Matters: Hearing before the S. Comm. on Armed Servs*., 114th Cong. 45 (2016) (statement of Sen. John McCain).

50 Ellen Nakashima, *Pentagon and Intelligence Community Chiefs Have Urged Obama to Remove the Head of the NSA*, Wash. Post (Nov. 19, 2016), https://www.washingtonpost.com/world/national-security/pentagon-and-intelligence-community-chiefs-have-urged-obama-to-remove-the-head-of-the-nsa/2016/11/19/44de6ea6-adff-11e6-977a-1030f822fc35_story.html.

51 *Id*.

52 Press Release, White House, Office of the Press Sec'y, Press Conference by President Obama in Lima, Peru (Nov. 20, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/11/20/press-conference-president-obama-lima-peru.

53 Press Release, White House, Office of the Press Sec'y, Statement by the President on Signing the National Defense Authorization Act for Fiscal Year 2017 (Dec. 23, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/23/statement-president-signing-national-defense-authorization-act-fiscal.

54 National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, Div. A, Title IX, § 923(a), 130 Stat. 2000, 2357 (2016).

55 2014 House Hearings, *supra* note 30, at 3 (written statement of Gen. Alexander).

56 Warner, *supra* note 19, at 131.

57 Warner, *supra* note 3, at 16.

[58] *Hearing to Consider Pending Nominations of Gen. Paul J. Selva & Vice Admiral Michael S. Rogers: Hearing before the S. Comm. on Armed Servs*., 113th Cong. 15 (2014) (statement of Gen. Paul J. Selva, US Air Force).

[59] Warner, *supra* note 3, at 16.

[60] Amber Corrin, *Fighting to the New Norm at Fleet Cyber Command*, C4ISR & Networks (May 8, 2014), https://web.archive.org/web/20140702005858/http://c4isrnet.com/article/20140507/C4ISRNET07/305070008/Fighting-new-norm-Fleet-Cyber-Command.

[61] Sean Lyngaas, *Sending Cyber Sense Down the Navy Chain of Command*, FCW (May 6, 2014), https://fcw.com/articles/2014/05/06/navy-cybersecurity.aspx.

[62] *U.S. Military Says Using Cyber Capabilities against Islamic State*, Reuters (Apr. 12, 2016) (describing Deputy Secretary Work as stating that "U.S. and coalition forces were putting pressure on Islamic State from all directions, using every possible military capability, including cyber attacks, to defeat the group"), https://www.reuters.com/article/us-mideast-crisis-usa-idUSKCN0X92A6.

[63] Ash Carter, Belfer Center, A Lasting Defeat: The Campaign to Destroy ISIS 33 (2017).

[64] Joseph L. Votel, David J. Julazadeh, and Weilun Lin, *Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR*, 3 Cyber Def. Rev. 18 (2018), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1716428/operationalizing-the-information-environment-lessons-learned-from-cyber-integra/.

[65] Gen. Townsend was then commander of Army Training and Doctrine Command, and he spoke to the Association of the US Army. *See* Mark Pomerleau, *Army Leaders Need More Payoff from Cyber*, Fifth Domain (May 24, 2018), https://www.fifthdomain.com/dod/2018/05/24/army-leaders-need-more-payoff-from-cyber/.

[66] Carter, *supra* note 63, at 33.

[67] Votel et al., *supra* note 64, at 18.

[68] Dina Temple-Raston, *How the U.S. Hacked ISIS*, NPR (Sept. 26, 2019), https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

[69] *Id*.

[70] US CyberCom, USCYBERCOM 120-Day Assessment of Operation Glowing Symphony 3 (2017), https://nsarchive.gwu.edu/dc.html?doc=6655597-National-Security-Archive-6-USCYBERCOM.

[71] The same document states that a new process was in place by November 22. US CyberCom, Operation Glowing Symphony: J3 AAR Observations (2016), https://nsarchive.gwu.edu/dc.html?doc=6655595-National-Security-Archive-4-USCYBERCOM-Operation.

[72] Shannon Vavra, *Top Secret Documents Show Cyber Command's Growing Pains in its Mission Against ISIS*, CyberScoop (Jan. 21, 2020), https://www.cyberscoop.com/cyber-command-pentagon-counter-isis-glowing-symphony-foia/.

[73] Temple-Raston, *supra* note 68.

[74] *Id*.

[75] Stephanie Borys, *Licence to Hack: Using a Keyboard to Fight Islamic State*, ABC [Australian Broadcasting Corporation] (Dec. 17, 2019), https://www.abc.net.au/news/2019-12-18/inside-the-islamic-state-hack-that-crippled-the-terror-group/11792958?nw=0.

[76] *The Fiscal Year 2021 Budget Request for US Cyber Command and Operations in Cyberspace: Hearing before the H. Comm. on Armed Servs., Subcomm. on Intelligence, Emerging Threats and Capabilities*, 116th Cong. 47 (2020) [hereinafter 2020 House Hearings] (statement of Gen. Paul M. Nakasone, Commander, US Cyber Command).

[77] US CyberCom, USCYBERCOM 30-Day Assessment of Operation Glowing Symphony (2016), https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM.

[78] *Id*.

[79] Votel et al., *supra* note 64, at 18.

[80] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1632, 132 Stat. 1636, 2123–24 (2019) (stating that a "clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 USC. § 3093(e)(2))").

[81] *See id.* § 1642.

[82] Dustin Volz, *White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons*, Wall Street J. (Sept. 20, 2018), https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729.

[83] US Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command 6 (2018).

[84] William T. Eliason, *An Interview with Paul M. Nakasone*, 92 Joint Force Q. 5 (2019).

[85] 2020 House Hearings, *supra* note 76, at 28 (statement of Kenneth Rapuano, Assistant Sec. of Def. for Homeland Def. and Global Sec. and Principal Cyber Advisor).

[86] Indictment, *United States of America v. Internet Research Agency LLC*, No. 1:18-cr-00032-DLF (D.D.C. filed Feb. 16, 2018); *see also* Scott Shane, *These Are the Ads Russia Bought on Facebook in 2016*, N.Y. Times (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

[87] Deputy Att'y Gen. Rod Rosenstein, Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election through Computer Hacking and Related Offenses (July 13, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-announcing-indictment-twelve.

[88] Ellen Nakashima and Paul Sonne, *Bolton Says US Is Conducting 'Offensive Cyber' Action to Thwart Would-Be Election Disrupters*, Wash. Post (Oct. 31, 2018), https://www.washingtonpost.com/world/national-security/bolton-acknowledges-us-has-taken-action-to-thwart-would-be-election-disrupters/2018/10/31/0c5dfa64-dd3d-11e8-85df-7a6b4d25cfbb_story.html; *see also* Ellen Nakashima, *White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries*, Wash. Post (Sept. 20, 2018), https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

[89] 2020 House Hearings, *supra* note 76, at 46 (statement of Gen. Nakasone).

[90] David Ignatius, *The US Military Is Quietly Launching Efforts to Deter Russian Meddling*, Wash. Post (Feb. 7, 2019), https://www.washingtonpost.com/opinions/the-us-military-is-quietly-launching-efforts-to-deter-russian-meddling/2019/02/07/4de5c5fa-2b19-11e9-b2fc-721718903bfc_story.html.

[91] *Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program: Hearing before the S. Comm. on Armed Servs.*, 116th Cong. 19, 20 (2019) (statement of Sen. Richard Blumenthal).

[92] 2020 House Hearings, *supra* note 76, at 46 (statement of Gen. Nakasone).

[93] *Id*. at 34 (statement of Assistant Sec. of Def. Rapuano).

[94] Paul M. Nakasone and Michael Sulmeyer, *How to Compete in Cyberspace: Cyber Command's New Approach*, Foreign Aff. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[95] Temple-Raston, *supra* note 68.

[96] 2020 House Hearings, *supra* note 76, at 45 (statement of Gen. Nakasone).

[97] *Id*. at 46.

[98] David Sanger and Julian Barnes, *U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came*, N.Y. Times (Nov. 9, 2020), https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.

[99] Temple-Raston, *supra* note 68.

[100] Nakasone and Sulmeyer, *supra* note 94.

[101] 2020 House Hearings, *supra* note 76, at 43 (statement of Gen. Nakasone).

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The views expressed in this essay are entirely those of the author and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

The preferred citation for this publication is Michael Warner, *US Cyber Command's First Decade*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2008 (December 3, 2020), available at https://www.lawfareblog.com/us-cyber-commands-first-decade.

About the Author

MICHAEL WARNER

Dr. Michael Warner is command historian at United States Cyber Command. He and John Childress recently published *The Use of Force for State Power: History and Future* (Palgrave Macmillan, 2020).

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION