Building a New Command in Cyberspace

Cybersecurity is vital to our nation. Part of our task at US Cyber Command is ensuring that our nation understands what it is that the White House, Congress, and the Department of Defense have charged us to do and why it is so important that it be done well. Constructing a new command while conducting operations is quite a challenge, especially in a time of rapid technological and policy changes, but this new command has produced results that have made our nation stronger and more secure and has already returned cybersecurity dividends on the investments of time and resources dedicated to its creation.

The Road to Full Operational Capability

US Cyber Command achieved full operational capability (FOC) on 31 October 2010 as a subunified command under US Strategic Command (USSTRATCOM). The road to FOC culminated roughly according to the timetable prescribed by the secretary of defense when he directed the establishment of the command back in June 2009. Initial operational capability (IOC) was originally projected to have been reached that October, but that date slipped to May 2010, when my nomination to serve as its first commander was confirmed by the Senate. We put the months between October 2009 and May 2010 to good use, however, building a consolidated staff to merge the two legacy organizations, Joint Functional Component Command for Network Warfare (JFCC-NW) and Joint Task Force for Global Network Operations (JTF-GNO), which together became Cyber Command. We also outlined the tasks needed to move us to FOC once the clock started running. Though the interval between initial capability in May and attaining full operational capability in October was only five months instead of the planned 12, we were able to attain several goals. Moreover, we did so while accelerating the tempo of daily operations that had been established by JTF-GNO and JFCC-NW.

Editor's Note: In March 2011 GEN Keith B. Alexander, USA, testified before the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities on the progress made in establishing US Cyber Command. This commentary reflects his statement on that occasion.

Despite the compressed schedule, the consolidated staff at Cyber Command accomplished a great deal by October 2010. We established a joint operations center, transferred operational control of the JTF-GNO mission set to Fort Meade, Maryland, and stood down JTF-GNO's 24/7 watch center in Arlington, Virginia; these steps helped USSTRATCOM disestablish JFCC-NW and JTF-GNO. The latter task took a considerable amount of planning and careful orchestration because JTF-GNO's activities and workforce had to be transitioned from Northern Virginia to Fort Meade, while ensuring that the daily functioning of the DoD information networks continued unimpaired. We established effective operational command and control processes for the consolidated mission sets. A joint intelligence operations center was established. Our service cyber components were formally assigned to USSTRATCOM, and we continued building relationships with key partners. We embedded liaison officers at the combatant commands and set conditions to expand their presence in larger cyber support elements. We deployed expeditionary teams to support operations in Iraq and Afghanistan. We also made progress in our support of operational planning by the combatant commanders and in building processes for them to issue requirements for cyber support. The command accomplished all of this without negative mission impact, keeping the department's operations secure while making the transition transparent to users of its information systems.

The command's fiscal year 2012 budget is projected to be $159 million, and our workforce at that point is slated to be 464 military personnel and 467 civilians, for a total of 931 employees. This team's overall mission is to plan, coordinate, integrate, synchronize, and conduct activities to direct the operations in defense of specified DoD information networks and be prepared, when directed, to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure US and allied freedom of action in cyberspace, and deny the same to our adversaries. Last but not least, US Cyber Command continues to build synergy with the National Security Agency (NSA) to take advantage of the NSA's infrastructure and expertise, which remain crucial to our progress. Our collocation with the NSA allows the government to maximize our collective talent and capabilities.

Current Perspectives

Our leaders from President Obama on down have spoken of the importance to our nation of preserving our security in cyberspace and maintaining

our freedom of action in this new, unique, man-made domain. We face many challenges in doing so, especially in light of recent developments.

The cyber threat continues to evolve, posing dangers that far exceed the 2008 breach of our classified systems that Deputy Secretary of Defense William Lynn described in his Fall 2010 *Foreign Affairs* article as a turning point for cybersecurity. Our nation now depends on access to cyberspace and the data and capabilities residing there; we are collectively vulnerable to an array of threats ranging from network instability, to criminal and terrorist activities, to state-sponsored capabilities that are progressing from exploitation to disruption to destruction. While we have not suffered disastrous or irreparable harm in cyberspace from any of these risk categories, we must be prepared to counter these threats.

Both external actors and insider threats pose significant challenges to our cybersecurity. No state actor, of course, has admitted to launching disruptive cyber attacks on another state. Yet incidents have occurred that look a great deal like such attacks. The cyber assaults on Estonia in 2007 spurred the United States and our NATO allies to deliberate regarding what in cyberspace would constitute an "armed attack" on an alliance member that would trigger the North Atlantic Treaty's provisions on collective defense. The following year, the invasion of Georgia coincided with precisely targeted cyber attacks, marking one of the first times we have seen such "cyber supporting fires." The coincidence was so perfect that independent observers concluded there was no coincidence—that the hackers who temporarily crippled the Georgian government's response and communications with the outside world had practiced their assaults and responded to official cues when they mounted them for real.

We have recently seen Internet access manipulated or curtailed by governments to suppress and disrupt even peaceful protests by their own citizens. In addition, we believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are proliferating into national arsenals and possibly beyond, moving them a step closer to intentional use or accidental release. Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.

We also watch with concern the growing capabilities of nonstate actors. The threats we see here are asymmetric, meaning that comparatively new

or lesser players can cause effects commensurate with state-sponsored actions. Although individuals with computer skills have independently shown that such attacks can be launched by even a lone actor with a laptop and a motive, we are chiefly focused on terrorists and well-organized cyber criminals. The former continue to grow more proficient in using the Internet as a medium for recruitment, coordination, and other activities, and they are becoming ever more sophisticated in doing so. Cyber criminals are more interested in the theft and exploitation of sensitive data that can bring them a profit, either directly through fraud or identity theft, or indirectly through the pirating of intellectual capital. Indeed, observers such as Senator Sheldon Whitehouse and a bipartisan team of colleagues last summer called this "the biggest transfer of wealth through theft and piracy in the history of mankind"—a transfer that has significantly lowered the cost for potential adversaries to close and counter our technological lead. Such activity is crime, of course, and belongs more properly in law enforcement than military channels, but when a prime target of such crime is our defense industrial base, we in the Department of Defense have a role to play in the response. We also find that state actors and terrorists can exploit the breaches and tools made by criminals, much as a dangerous pathogen opportunistically employs a disease vector to enter a host. Indeed, sometimes state and nonstate actors collaborate on matters of mutual interest.

Significant security challenges also emanate from poor cyber hygiene, inadvertent misuse, and malicious actions. After all, even the most astute malicious cyber actors—those who can break into almost any network that they really try to penetrate—are usually searching for targets of opportunity. They seek easy vulnerabilities in our system's security and then exploit them. Our own neglect thus makes us vulnerable. Unapplied software patches, firewalls left unattended, and antivirus suites that never get updated even in the US military cause us serious trouble, especially when a risk to one is a risk shared by all. Now multiply those problems across the government and the private sector, and realize that we have networked our vulnerabilities while segmenting our defenses among the .mil, .gov, .com, and .edu Internet domains. Each domain (and often each system) has been left to fend for itself against cyber actors who care little for legal distinctions and organizational boundaries. And finally there is the insider threat; some of the largest security breaches in history have originated from the inside.

The recent creation of Cyber Command has garnered a great deal of interest from foreign militaries and the governments that oversee them. We see frequent media reports on nations contemplating the creation of their own "cyber commands." This appears to be a sign not necessarily of a "militarization" of cyberspace but rather a reflection of the level of the concern with which civilian and military leaders around the world are viewing current problems. Many such steps are essentially defensive, and if so many nations are interested in improving their defenses, they might be more willing to talk about ways they can reduce common threats. There is a rough, de facto deterrence at the strategic level of cyberspace. Although no one knows how a cyber war would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way. This concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects. Lest optimism obscure real threats, however, we must note that we have no certain capability to restrain the behavior of radical, non-state extremists.

In sum, our adversaries in cyberspace are highly capable. Our economy and society have become directly or indirectly dependent on access to and freedom of movement in cyberspace—and indeed our military is equally dependent on such access—and thus we cannot be content with a situation in which we are sometimes our own worst enemy.

Working toward the Future

US Cyber Command's efforts and planning aim to ensure that the DoD has done all it can to defend and deter determined adversaries, mitigate dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation's equities in cyberspace is a losing proposition.

Our command faces serious challenges as it comes together to do urgently needed work in cyberspace. Its establishment reflects the department's need to manage cyber risk, secure freedom of action, and ensure the development of integrated capabilities. Our intent is to overcome the challenges we face through the concerted efforts of implementing the department's recently approved strategy for cyberspace. We will pursue resolution of the capacity, resources, and information technology efficiencies issues we face through the five strategic initiatives of that strategy. We intend to:

- treat cyberspace as a domain for the purposes of organizing, training, and equipping, so the DoD can take full advantage of its potential in military, intelligence, and business operations;
- employ new defense operating concepts, including active cyber defenses such as screening traffic, to protect DoD networks and systems;
- partner closely with other US government departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cybersecurity;
- build robust relationships with US allies and international partners to enable information sharing and strengthen collective cybersecurity; and
- leverage the nation's ingenuity by recruiting and retaining an exceptional cyber workforce and enable rapid technological innovation.

Our first duty is to ensure that DoD networks are secure. Doing so is crucial to protecting our data, to maintaining our war-fighting potential, and ultimately to defending our nation. Until recently we all viewed our networks as a great force multiplier—the magic that let us put ordnance on target and dispatch planes, troops, and ships to where they were needed, when they had to be there. Today, however, we understand that those networks represent a serious vulnerability, and we dread the thought of someone getting inside to bring them down or, perhaps even worse, to make a few subtle changes to the integrity of our data that will bring all our military operations to a halt. Without fast, assured, and safe data flows, we will not be able to fight our adversaries in the way we as Americans think they should be fought. We are not necessarily close to losing that edge, but potential adversaries understand where it lies, and are certainly contemplating ways of blunting it in any future conflict.

US Cyber Command is working to preserve that information advantage in many ways. We are directing the operations of the department's information networks, which knit together seven million computing devices spread across fifteen thousand networks. The recent move of the Defense Information Systems Agency (DISA) to a new facility on Fort Meade has enabled even greater collaboration between our two organizations. Cyber Command and the DISA collaborate on a daily basis to monitor the functioning of DoD information networks. That work includes the maintenance of sensors to detect and block adversary activity in those networks, the inspection of security settings and practices, and

the investigation of real and suspected incidents. Together we are making progress in all of these areas, growing our ability to stop intrusions and adapt to changing adversarial practices almost as fast as they evolve. The new sensor capabilities we are deploying and the aggressive inspection regime now coming together will improve our situation even more.

We also plan—in partnership with the NSA—the defense of specified DoD information systems, knowing that we have to stay ahead of the cyber threat in technological terms. Here US Cyber Command and our partners in the department are working on ways of shifting to a different and more defensible architecture for providing information services to users. A year from now we should be well on our way to having a hardened architecture proven, deployed, and providing a new level of cybersecurity. The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of "cloud" computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use—each of which has to be individually secured—up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter. Moving to a cloud architecture has the advantages of producing economies of scale and reducing the department's information technology costs. This architecture also would seem at first glance to be vulnerable to insider threats—indeed, no system that human beings use can be made immune to abuse—but we are convinced the controls and tools that will be built into the cloud will ensure that people cannot see any data beyond what they need for their jobs and will be swiftly identified if they make unauthorized attempts to access data.

Over the next year we hope to "operationalize" our department's networks. We will, of course, continue to do this with full regard for and protection of the privacy and civil liberties of all Americans as well as in compliance with all applicable laws and regulations. The idea is to transform DoD information systems from something to be passively guarded into a suite of capabilities that offer our commanders and senior leaders opportunities to adjust our defenses. If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready.

Our command's mission document states that we coordinate, integrate, and synchronize activities to direct the operations and defense of DoD

networks. In practice, that means we spend a great deal of time talking with leaders and experts in the department, the US government, private industry, and other nations as well. This effort begins, of course, with US Cyber Command's service cyber components, which provide the forces that implement our plans and execute our directives—Army Cyber Command, Marine Corps Forces Cyber Command, Fleet Cyber Command, and Air Force Cyber Command. We are still maturing the ways in which we and they will interact to support and be supported by the geographic combatant commands in various situations. Our mission depends as well on the work of the NSA, which provides the expertise and intelligence that are indispensable to understanding what is happening in cyberspace. We are constantly engaged with the DISA as well, and our relationship with it will likely change substantially and become even closer in the near future.

We have also strengthened our strategic partnership with the Department of Homeland Security (DHS) in accord with the recent agreement concluded by Secretaries Robert Gates and Janet Napolitano. A senior DHS official now works at the NSA with us, leads a DHS–DoD joint coordination element that was also established by the agreement, and attends many of our leadership meetings. Several government agencies are also represented 24 hours a day in our joint operations center. These measures, along with complementary measures at the DHS and other partners, should provide a whole-of-government awareness of what everyone is seeing so that we can plan for and execute authorized and coordinated joint actions in the event of an emergency. Finally, we are active players in the Defense Department's productive discussions between government and industry over how to share information regarding common threats and potential ways of mitigating them. The vast majority of our military's information rides on commercial infrastructure, and thus we need to develop shared insights into those dependencies for mission assurance purposes.

The second part of our mission at Cyber Command is to be prepared to conduct full-spectrum military cyberspace operations to enable actions in all domains. As I noted above, state and nonstate actors have already experimented with ways to harass or attack rival governments, whether to make a strategic point or in conjunction with kinetic attacks. Our military and our nation would be unwise to assume that we have seen the last of such attacks. We are prepared, when directed and in full compliance with applicable laws, to respond when we or our allies are threatened or subjected

to the use of force in the cyberspace. The president has emphasized that our digital infrastructure is a strategic national asset and has insisted that preparing our government for the task of protecting strategic national assets in cyberspace is a national security priority. Our efforts to do this are designed to achieve two goals:

- First, we protect US and allied freedom of action in cyberspace. It is no longer possible to conceive of our nation functioning properly or even defending itself without the ability to create, transmit, and secure masses of digitized data. Making our access to cyberspace impossible or even problematic would represent a strategic threat to America's vital interests—one that our command has been established and tasked to prevent with respect to DoD operations in cyberspace. Furthermore, our cybersecurity is inextricably linked with that of our allies, and our interests in cyberspace can also coincide with those of other states with whom we have less-formal ties. The lack of geographic borders in cyberspace means that a threat to one can be a threat to all, which gives us a real incentive to share situational awareness and best practices that help to protect our military, government, and private networks and data.

- Second, when directed, we need to deny freedom of action in cyberspace for our adversaries. As with all activities the DoD pursues, operations are only executed with a clear mission and under clear authorities, and they are governed by all applicable laws, including the law of armed conflict. We cannot afford to allow cyberspace to be a sanctuary where real and potential adversaries can marshal forces and capabilities to use against us and our allies. This is not a hypothetical danger; in conflict areas where US forces are engaged we have indeed seen the Internet used for recruiting, fundraising, operational training, and other activities directed against our service personnel and coalition partners. At Cyber Command much of our focus is on helping our troops in the field limit their vulnerabilities in and from cyberspace. This effort reflects the likelihood that, henceforth, all conflicts will have some cyber aspect, and our efforts to understand this development will be crucial to the future security of the United States.

Conclusion

The Department of Defense took an important step for our nation in creating US Cyber Command and declaring it to be fully operational capable. At Cyber Command we have a mission to actively manage the department's information networks—not just to defend them but also to use them as a tool to assist our warfighters, planners, and commanders by preserving their freedom of action—and also to be as ready to use our own capabilities to disrupt any adversarial use of cyberspace against US interests. The command is seeking to:

- increase the capacity of the cyber workforce;
- implement and exploit, in a strengthened partnership with NSA, the transformation of the department's networks;
- work with the combatant commands to synchronize processes and planning to deliver the joint effects they require;
- extend cyber defense capabilities across US government networks through supporting partnerships with the NSA and the DHS as it works to secure federal, civilian, non-national security systems; and,
- with the DHS, increase government dialogue with private partners on the protection of our nation's critical infrastructure.

US Cyber Command operates with respect for civil liberties and in compliance with the laws governing the privacy of our fellow Americans, in accord with the directives of the national command authority, and in conjunction with mission partners in the Departments of Defense and Homeland Security, law enforcement, the intelligence community, industry, and academia. We do not see the security of our nation and the protection of civil liberties and privacy as a "balance"; rather, we believe we can and must defend both. I am confident that together we will succeed.

GEN Keith B. Alexander, USA
Commander, US Cyber Command
Director, National Security Agency
Chief, Central Security Service