National Defense and the Cyber Domain

G. Alexander Crowther, PhD

What is "cyberspace," and how does it relate to military affairs? "Cyberspace" is a term that is constantly used but seldom well defined. Its characteristics are poorly understood in the larger public discussion, especially with regard to national security and military matters. This is unfortunate because "cyber" has become profoundly central to nearly everything the military does in defense of U.S. national security interests.

As a domain through which actions can be taken instantaneously, globally, and even anonymously, cyberspace provides opportunities and challenges to countries, groups, and individuals unlike those presented by any other domain or capability. Cyberspace provides someone with the ability to attack anywhere, at any time, with a keystroke. There is no need to deploy a physical force, gain physical access to a region (otherwise done by ship, plane, or overland movement), or be encumbered by mounds of equipment and supplies. An attacker acts in absolute silence, perhaps visible only to the most skilled cyber defender. There is no need to limit one's force to specific ages, physical conditions, or body size, nor is there a need for sprawling bases, expensive facilities (like ports or airfields), square miles of training areas, extensive stockpiles of munitions, or assured access to fuel.

Cyber is generally not affected by environmental concerns or weather conditions. To the extent that cyber operations can be fully automated, they can be undertaken relentlessly, without regard for time, periods of rest, or any other constraint related to the normal use of people and equipment. In short, cyberspace provides a virtually unconstrained sphere through which nearly anyone can act against almost any target without concern for the physical impediments and resources that accompany physical actions.

A wide variety of actors operate in cyberspace. The government of the United States has a variety of responsibilities to the American public, but precisely where the responsibility lies and the extent of that responsibility are currently subjects of debate. Although 90 percent of the Internet traffic in the U.S. is in the private sector,[1] cyberspace is one place for which the U.S. government has acknowledged responsibility. Working mainly through the Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Justice (DOJ):

> The United States will work to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, [the U.S.] will build and sustain an environment in which **norms of responsible behavior** guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[2]

Cyberspace

Cyberspace has three layers: the physical network, the logical network, and the cyber persona.

- **The physical network** consists of the hardware, such as cables and your computer, and exists all around the world. Because it exists inside states, states have sovereignty over its components, and they must obey the laws of the states in which they reside.

- **The logical network** is the software that operates the network as well as its manifestations, such as a web page. These electrons that make up the logical network bounce around the globe, following the quickest route from one place to another, and route through hardware that is physically located in states. Some states, such as China and Russia, believe that they have sovereignty over this aspect of the cyber domain as well.

- **The cyber persona** is made up of the people who are operating in cyberspace. Like the physical network, they are present within states and subject to their laws and policies.

Colloquially, these three components are known as hardware, software, and wetware.[3]

The cyber domain has effectively penetrated the world's advanced economies and is making headway in the rest of the world. Many places in Africa, for instance, have skipped over the land line and gone straight to smart phones; currently, approximately 3.74 billion people are connected to the Internet.[4]

This connectivity provides a number of opportunities and challenges. It enables actions by both states and individuals across all of the elements of national power: diplomacy, information, the military, and the economy. It makes diplomatic activity more effective, for example, linking embassies and capitals with almost instant communications and allowing for better research. In addition, the opportunities that cyberspace provides for information are almost unlimited. Humankind creates huge amounts of information annually, and individuals and organizations are constantly digitizing old information, making it available to everyone.

Militarily, cyberspace allows for global command and control of forces and operations and the functioning of a globally distributed logistics system without which modern military operations would be impossible. Intelligence communities, commanders, and warfighters alike benefit from the uninterrupted flow of information. Economically, cyberspace has led to a global boom, from the technology giants Google and Amazon to the individual fisherman in India who can now determine where to obtain the best price for his catch.

In short, with its low barrier to entry, cyberspace has provided advantages across the globe and across the elements of national power. And these advantages grow as access to cyberspace spreads.

At the same time, cyberspace creates challenges. Wikileaks has revealed to the world stolen U.S. diplomatic communications, embarrassing the United States, irritating friends, and empowering enemies. Information is harder and harder to secure and easier and easier to steal. Economically, cyberspace has enabled criminals: Cyber crime cost the U.S. $100 billion and the global economy $400 billion in 2015, and the total is projected to reach $2 trillion by 2019.[5] For the U.S. military, compromise of the U.S. global command and control capability can be turned against the Department of Defense, frustrating or even preventing the execution of military operations.

Vulnerabilities and Actors

The U.S. has begun to confront challenges to its major interests in cyberspace: protection and enhancement of the economy, secure command and control of national defense assets, reliable collection of cyber intelligence, and protection of cyber intelligence and information.[6]

Three major groups threaten U.S. national security: people, states, and non-state actors. People include the general population, leaders, workers in nearly all business sectors, and insider threats. States primarily include Russia, China, Iran, and North Korea. Non-state actors include proxies, hacktivists, and criminals who sometimes work for themselves but also may work in support of others.

The Human Dimension. Humans are the weakest link in the cybersecurity system.[7] Unlike the physical world, in which potential human activity is limited by geographic and space limitations—Israel, for example, uses a barrier to keep out potential terrorists, and people do not own nuclear weapons or aircraft carriers—barriers to entry for cyber are so low that they have democratized cyber activity. Everyone who has a desktop, laptop, or smart phone is an actor and a potential problem. Because the only thing that organizations do well is what their leaders demand of them, leaders can be a key vulnerability, and thus a "threat" to their organizations, by not emphasizing cybersecurity. Workers using poor cyber hygiene are a threat. Gullible people or people with preconceived but flawed notions of safe cyber practices will fall prey to cyber crime or propaganda. Insiders who do not support their organizations are another threat.

The Population. People are the most vulnerable to cyber operations. Because many people engage in commercial transactions online and use social media daily, they are the most exposed to these varied threats. In general, people usually have not received training or education that would enable them to deal with varied cyber threats. Additionally, most people do not see their information as having value.

Leaders. Research supporting the 2014 Chairman of the Joint Chiefs of Staff war game *Iron Crucible* identified "understanding" as the major challenge in the 21st century.[8] Because most senior leaders typically are not involved in the information business, there is a wide variation in their knowledge of or insistence on best practices in the cyber domain.

The U.S. Office of Personnel Management (OPM) hacks of 2015 are a telling example of poor leadership in this area. Although OPM's Assistant Inspector General for Audits indicated that security shortfalls were well known, having been publicly acknowledged since 2007, the OPM Director did not make cybersecurity a priority. By the time the hacks were identified in 2015, nearly a quarter of OPM's information technology (IT) systems, including several of their most critical and sensitive applications, were operating without a valid cyber-certificate authorization.[9] If the Director had understood the implications of basic security shortfalls, perhaps the theft of sensitive personal information on over 22 million Americans could have been prevented.[10]

Senior officials are often the targets of cyber-attacks because they have access to more information, IT bends the rules for them, and the damage and financial payoff for the attacker can be much bigger.[11] Hence, senior leaders need more training and education to understand how to operate their systems, how to lead and manage cyber systems and workers, and how to decrease their own vulnerability. Senior leaders also need to integrate information activities into their day-to-day operations, whether it is in a business, government, or the military. Only when senior leaders understand the implications of cyberspace will they be able to address vulnerabilities and achieve synergies that cyberspace provides.

Workers. In a phishing quiz, 80 percent of participants misidentified at least one phishing e-mail.[12] Workers are a favorite target because the chance of success goes up when more people are targeted. Roughly 20 percent of trained workers will click on a phishing link[13] even if they have been trained not to do so.

Insider Threats. These involve a variety of motivations and are very difficult to identify ahead of time. Edward Snowden and Bradley Manning are well-known cases in the U.S. The Computer Emergency Response Team (CERT) Insider Threat Center at Carnegie Mellon University maintains a database of more than 1,000 insider threat cases and provides analysis and support to organizations working to prevent insider threats.[14] Another type of insider threat is the "Lone Wolf" or "Wolf Pack." These are individuals or groups that have been radicalized, typically through cognition-shaping cyber operations.

State Threats. Included in this category are threats posed by Russia, China, Iran, and North Korea. States can leverage enormous funding, the ability to organize, and the ability to coordinate actions (multi-domain and multi-tool) at levels far above that of an individual or small group. These state actors challenge the U.S. economy with brazen cyber espionage into critical U.S. companies.

In 2014, for example, a grand jury in the Western District of Pennsylvania indicted five officers from the Chinese People's Liberation Army for cyber espionage in support of state-owned enterprises (SOEs).[15] An array of cyber actors also has challenged the ability of the U.S. to secure its command and control of national security networks reliably and to secure its sensitive and personal information data. In 2015, Russians hacked the Joint Staff,[16] and the OPM discovered a Chinese hack of tens of millions of files containing sensitive personal data.[17] Additionally, the Russians have returned to their Cold War practices of aggressive information operations seeking to undermine developed countries[18] as well as international organizations.[19]

Iran and North Korea are second-tier threats for the United States, and both countries are continuously performing cyber operations against economic and government targets in the U.S. In 2016, the DOJ indicted seven Iranian hackers for operating against a dam and banks in the U.S.,[20] and North Korean hackers have been involved in stealing both money and military designs.[21]

Non-State Actors. This category includes threats from proxies, hacktivists, and criminals. Proxies work on behalf of a government that seeks cyber effects without paying a political price, hoping to achieve plausible deniability by outsourcing such work to individuals. The Russians often use criminals as proxies,[22] and the Chinese use other groups that may or may not be affiliated with each other or other similar criminal entities.

Hacktivists will perform a wide range of operations. Much like the difference between terrorists and freedom fighters, hacktivists attack you while patriots attack people you don't like. Ironically, some groups like Anonymous will attack anyone with whom they disagree, regardless of the target's politics.

Criminals operate across the world. As noted, it is estimated that cyber crime cost the U.S. $100 billion and the global economy $400 billion in 2015 and that the total will rise to $2 trillion by 2019.[23]

All of these actors are aided by the fact that it is very difficult to attribute cyber operations to a specific actor. Cyber actors take very specific steps to prevent attribution, typically by manipulating data to pretend to be someone else. This is one of the largest barriers to cybersecurity as it is difficult to deter an actor whose identity you can't prove.

Nature of Competition in Cyberspace

Competition in cyberspace is fierce and ongoing. States seek to undermine the global order to their own advantage. Individual actors and organizations seek to advance their own political agendas. Criminals seek to make illegal financial gains from cyberspace.

All of these can be inimical to the goals of the United States and its allies and partners. Russia seeks to use cyber-enabled information operations to sow discord inside and among the states that are trying to keep Russia at bay in Europe; China uses cyberspace to steal secrets that it can use for economic gain or to avoid the research and development costs (in time and money) for important military systems; Iran seeks to weaken its opponents around the world; and North Korea maneuvers in cyberspace to avoid international sanctions.

Because of the low barrier to entry into cyberspace and the potential gains to be made, the scale of the challenge is large and growing. The U.S. and its allies and partners need to safeguard their own government spaces, their economic activities, and their citizens. Although the U.S. has strengths including a wide variety of resources and a large, educated workforce, these bad actors use cyberspace to challenge the U.S. at every turn. The U.S. is having a hard time using traditional strengths (such as military power) against cyber actors.

The U.S. Government in Cyber

Because the U.S. government has a wide variety of resources and the obligation to safeguard the American population, the executive branch performs many cyber activities to mitigate the foregoing threats. The three main U.S. government actors in cyberspace, as noted, are the Departments of Homeland Security, Justice, and Defense.

- **The DHS** coordinates the national protection against, prevention and mitigation of, and recovery from cyber incidents; disseminates domestic cyber threat and vulnerability analysis; protects critical infrastructure; secures federal civilian systems (the .gov domain); and investigates cyber crimes under its jurisdiction.
- **The DOJ** investigates, attributes, disrupts, and prosecutes cyber crimes; is the lead agency for domestic national security operations; conducts domestic collection, analysis, and dissemination of cyber threat intelligence; supports the national protection against, prevention and mitigation of, and recovery from cyber incidents; and coordinates cyber threat investigations.
- **The DOD** is charged with securing the nation's freedom of action in cyberspace and helping to mitigate risks to national security resulting from America's growing dependence on cyberspace. Specific mission sets include directing, securing, and defending DOD Information Network (DODIN) operations (including the .mil domain); maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; and providing support to civil authorities and international partners.[24]

Deterrence. Ongoing cyber operations against the United States demonstrate that the country has extremely limited capability to deter cyber operations, that the U.S. cyber deterrence threat is not credible, and that U. S. cyber deterrence is failing.[25]

Deterrence is designed to convince others not to perform certain tasks. In this case, it ideally should prevent other actors from performing all four types of cyber operations. One thing that can make cyber deterrence less effective, as noted, is the difficulty involved in attributing an operation to a specific actor. Additionally, second-order and third-order analysis to predict what ancillary actions would follow certain types of cyber-attacks is very difficult to perform in the cyber realm. Incorrect analysis could cause a deterrence operation to trigger a completely opposite reaction and accidentally escalate rather than deter, which causes second thoughts on allowing offensive cyber operations.[26]

The use of cyber capabilities to deter faces two major barriers: For deterrence to work, opponents must believe that they will pay a price for an action, and the target audience needs to understand who is deterring them. This in turn requires a credible threat. Opponents do not currently believe that they will face retaliation in response to their attacks on U.S. assets. Effective cyber retaliation requires that operators perform an attack and leave behind digital "fingerprints" identifying the originator or an explicit message naming the origin of the attack.

But this presents two further problems: Cyber operators do not want to compromise their capabilities by performing an operation that can be traced to them, and it has been difficult to receive clearance to perform offensive cyber operations (OCOs). Any OCO that has major effects can alert an opponent to the presence of intruders, which allows opponents to defend against the intrusion. It can also reveal cyber capabilities, which is anathema to the community that prizes its ability to work in secret. Moreover, it sometimes takes months to penetrate opposition cyber systems. Executing an attack will announce the operator's presence and "waste" the time required to penetrate and repenetrate target servers.

The Military Cyber Domain

The DOD does not define "domain," but it does define cyberspace as "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[27] The words "infrastructures and resident data" cover the physical and logical aspects of cyberspace but not the persona aspect. The use of "domain" is meant to indicate that cyberspace is now coequal with the other conventional domains: sea, air, land, and space.[28] This is intended to communicate to leaders within the DOD that they need to pay as much attention to cyber issues as they would pay to air, sea, land, and space issues.

There are four sets of cyberspace activities that pertain to the military: intelligence, information, crime, and military operations.[29] Although the military has equities in all of these areas, it predominates only in the military operations portion. However, there are aspects of intelligence, information, and criminal activities in cyberspace that do involve the military.

In any of these fields, there is a spectrum of activity that ranges from conventional to cyber-enabled to cyber-centric to pure cyber operations.

Normal intelligence operations like stealing secrets and developing sources would have been the traditional approach before the advent of cyberspace. Cyber-enabled intelligence operations would use cyber capabilities in support of these operations, such as analysis of a terrorist network using data that had been gathered by traditional intelligence means. Cyber intelligence operations would be operations that occur entirely in cyberspace, such as the 2012 operation by Chinese hackers that penetrated Indian Navy computers and compromised sensitive information.[30] Purely cyber operations would consist of information and communications technology, network, and defensive cyber operations.

Conventional criminal operations would be old-school crime, such as entering a bank with a pistol and a bag. Cyber-enabled criminal operations would fuse technology and crime, such as ATM-skimming, where criminals use hidden electronics to steal the personal information stored on bank ATM cards and record PIN numbers in order to access victims' accounts.[31] Cyber crime would be a criminal operation that occurs wholly in cyberspace, such as the use of the SWIFT system to steal $81 million from the Bank of Bangladesh.[32]

Conventional information operations would be old-fashioned propaganda or even advertising via printed text, radio waves, or television. The 2016 hack of the Democratic National Committee would be an example of a cyber-enabled information operation.[33] The information was obtained through cyber operations but released through Wikileaks.[34] Cyber information operations would include Daesh recruiting videos, an information operation that takes place entirely in cyberspace.

Military operations can also be cyber-enabled or executed purely in cyberspace. A normal military operation would be the invasion of Iraq. A normal special operation would be the raid to kill Osama bin Laden. An example of a cyber-enabled conventional military operation would be Russian operations in Georgia in 2008 when Russia conducted cyber operations against Georgian targets to degrade Georgian command and control in support of Russian conventional military operations on the ground and in the air.[35] An example of a cyber-enabled special operation would be the Mumbai attack of 2008. Planners used a GoPro camera while walking the route to be used in the attack so everyone could see videos of their routes before the operation. They also used Google Earth during their planning process. The command element monitored Indian social media and traditional media (such as radio and television) to track the response by Indian security forces and steered the ground force away from reacting Indian forces, enabling the operation to continue much longer than it would have normally.[36]

Cyber military operations include conventional and special operations. A conventional cyber operation would be like "dropping cyber bombs on Daesh." Secretary of Defense Ashton Carter explained at an event at NORTHCOM that "[w]e're using these tools to deny the ability of ISIL leadership to command and finance their forces and control their populations; to identify and locate ISIL cyber actors; and to undermine the ability of ISIL recruiters to inspire or direct Homegrown Violent Extremists."[37] This is a conventional operation in that it does not require special techniques or unique modes of employment in a covert nature.

A cyber special operation would be the Stuxnet attacks on Iran. This operation meets many of the criteria for a special operation as defined in the DOD's Joint Publication 3-05, *Special Operations*.[38] It required unique modes of employment, tactics, techniques, procedures, and equipment. It was conducted in a hostile, denied, or politically and/or diplomatically sensitive environment and was characterized by a clandestine or covert nature (no one has yet proved who conducted the operation) and low visibility.

Criminal operations do not usually pertain to militaries in the conventional sense. In cyberspace, however, there are crimes that involve members of the DOD, as well as crimes that involve the Defense Industrial Base. Additionally, members of the DOD participate in several types of activities that pertain to cyber crime and cyber-enabled crime, including cyber security and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.[39]

Each of these provides examples of how the military would be involved in four areas: crime, intelligence, information operations, and military operations. Although military forces are involved in these areas, they are not involved in all operations in these areas (the DOJ handles most cyber crime). This, then, is the circumscribed area that can be called the military cyber domain. These distinct categories are changing and becoming more integrated with cyber activities. As cyber capabilities expand, more military operations will be enabled by them; eventually all military operations will be enabled by cyber capabilities.

Military Cyber Operations

There are four main types of cyber operations: shaping cognition; cyber surveillance and reconnaissance (CSR); operational preparation of the environment (OPE); and cyberspace attacks. They can be either defensive or offensive in nature. Defensive cyber operations (DCOs) comprise the vast majority of U.S. government (and military) activities. Offensive cyber operations (OCOs) are rarer for the United States. None of these activities is unique to cyberspace. All military operations require reconnaissance and preparation, and shaping cognition through information (for example, through advertising) is ubiquitous in modern society.

Opponents perform shaping-cognition intelligence operations against the United States on a minute-by-minute basis and perform OPE regularly. Large-scale, destructive cyberspace attacks are rare but have the potential to be catastrophic in their effects.

Shaping cognition is using information to cause people to think in a certain way. This can be benign like Facebook or malign like cyber crime. It is perhaps the most significant opportunity and challenge for cyber today. Due to the pervasive nature of information in the 21st century, everyone who connects to the Internet can shape the thoughts of others. Radicalization by state and non-state actors is a significant challenge, especially lone-wolf or wolf-pack radicalization. The Islamic State has successful influence operations running globally 24 hours a day. The fact that volunteers have been to ISIS territory from around the world indicates how successful these operations are. Other actors target populations of other countries (to radicalize); government employees (to create an insider threat); and businesses (to coerce or blackmail them into behavior that the initiator desires). Governments consequently struggle to cope with widespread cognition shaping.

CSR is data gathering. Google gathers data every time one accesses the Internet. States gather data on people in other countries or on their own citizens. States such as China gather economic data and pass it on to their state-owned enterprises who use it to obtain a competitive advantage in the marketplace. Criminals gather data to better execute their criminal activities. Today, everyone is a data-gatherer.

OPE is specific preparation of the environment for follow-on operations by installing "back doors" in targeted computer systems so that they can return at a later time to execute an attack or devising specially designed software that will allow them to achieve an effect, such as opening the gates on a dam. Among recent examples, as noted, are the seven Iranians who were indicted for hacking into banks and a dam in New York.[40]

OCOs are a means by which to achieve an end, another tool that provides additional capabilities to the President and battlefield commanders and relevant forces.

Cyber operations are limited only by the imagination and capability of the attackers, yet there are only two types of cyber-attacks: syntactic and semantic.[41] Syntactic operations involve the actual coding used in a piece of cyber programming (the syntax of the coding), and semantic operations seek to shape thoughts using language or semantics. As an example, a phishing operation begins as a semantic operation, asking the target to "click on this link," and then, once the link is activated, changes to a syntactic attack by which the malicious code enters the target's system and changes the syntax of the code in the targeted platform. Shaping the thoughts of others may be the more important of these two types of attack.

A cyberspace attack produces two forms of effect: manipulation and denial. Manipulation means controlling or changing the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. Denial attempts to degrade, disrupt, or destroy. Degrading limits the capacity of a target, and disruption completely but temporarily prevents access to a target.[42] Destruction eliminates the target altogether.

Cyber operations are changing the characteristics of warfare. Although the nature of war is constant, the characteristics of warfare can change whenever a new weapon or tactical approach is introduced. Operations in cyberspace now allow for more information to be acquired and shared and better command and control to be exercised on the battlefield, theoretically decreasing the "fog of war" by adding fidelity to the commander's understanding of the battlespace. It allows for more accurate and effective use of the people and logistics capabilities involved, putting the right person or widget at the right place at the right time. It also allows for a significant improvement in the ability to shape cognition.

While it allows all of these to assist friendly forces, however, it also allows our opponents to do the same. They will have a better understanding of—and consequently an opportunity to copy or defeat—our technologies and capabilities. They will be able to access our command and control and logistics networks, potentially modifying orders so that forces or spare parts end up in the wrong place. They also will be able to use patterns in the movement of information to improve their own intelligence, identifying our units and their capabilities.

These capabilities require the U.S. government generally, as well as the U.S. military specifically, to modify its practices. Leaders and organizations need to do a better job of selecting and utilizing new technology. Laws and policies need to be updated to leverage the new technology. Older leaders need to understand how younger followers perceive and use technology.

Implications for Operations. Cyberspace permeates all aspects of our daily lives and therefore all operations whether military, governmental, or commercial. Cyber operations, including information operations, will require attention from leaders from the tactical level to the strategic level.

At the tactical or local level, cyber operations will provide information to the warfighter that previously did not exist or was available only to national-level leaders. Soldiers will carry smart phones, which will require command attention and supervision to prevent the unintentional compromise of militarily relevant information. Units will have access to huge amounts of information, including the position of every friendly vehicle, soldier, airframe, and ship as well as any enemy forces that have been identified. This information will make our forces much more effective and efficient if properly utilized.

At the same time, our opponents will use their similar capabilities as effectively as they can to accomplish their own objectives in keeping with their own integrated information warfare doctrine. It will be difficult for U.S., allied, and partner units to control their own information while exploiting their opponent's information. Units will have to perform DCOs at all levels. Failing to do so will likely result in operational paralysis when their command and control assets are degraded or destroyed. They also will have access to limited OCOs if their particular mission warrants access to that level of support.

Automation and information flows will make day-to-day operations easier. However, while attention to sound DCOs and skillful execution of OCOs will lead to military success, failure in each case will present exploitable opportunities to an enemy.

Implications for the Services. As occurred when airplanes, tanks, and automatic weapons were introduced to war, forces will need to reorganize to integrate robust cyber and particularly information capabilities. Specifically, the services will have to:

- **Modify** training and equipping to ensure that units practice DCO at all times and will have to stand up additional OCO capabilities as their use becomes more widespread.

- Because cyber operations happen at nearly instantaneous speed and in a wide variety of locations simultaneously, **modify** their doctrine to allow for greater authority to execute cyber operations at much lower and more local levels in order for units to continue to function when command and control are degraded and operate effectively at the speed of information.

- **Purchase** more modern information technology equipment and software, which are inherently more secure.

- **Provide** universal, entertaining, iterative cyber hygiene training to the entire force. Properly equipped and trained units will be able to be much more effective and efficient in information-age combat. According to the Australian Signals Directorate, 85 percent of cyber problems can be mitigated with proper cyber hygiene.[43] This will be expensive in the short term, but once it is fully integrated into the force, it will act as a force multiplier.

U.S. Military Cyber

The Office of the Secretary of Defense articulates three primary cyber missions: "**defend DoD networks, systems, and information**; **defend the nation against cyberattacks of significant consequence**; and **support military operational and contingency plans**."[44]

Because the DOD is a very large, bureaucratic organization that operates around the world, it is proving difficult for it to fully embrace cyberspace operations. First, there are DOD legacy structures. Services such as the Army provide trained and equipped forces, while Combatant Commands (CCMDs) like U.S. European Command (EUCOM) and U.S. Pacific Command (PACOM) use those forces for missions. This means that the DOD, the largest organization in the world, must simultaneously defend every military system that is linked in any way to or affected by "cyber" used by DOD, the Joint Staff, the three military departments, and four services that collectively employ almost 3 million people, more than 450,000 of whom work overseas, both afloat and ashore.

The department's responsibilities also include several hundred thousand individual buildings and structures located at more than 5,000 different locations or sites worldwide.[45] Each person in the DOD needs to communicate and pass information on a daily basis. Many have multiple computers and devices that they operate on different networks. All of this must be secure and reliable, from the Nuclear Command and Control System down to tactical radios that connect soldiers in the field.

Adding further complication, each service is responsible for its own procurement of computers, devices, and components and has its own procedures for doing so.[46] Each service defends itself, at least in part, and the DOD maintains separate organizations to defend the larger organization and defense agencies apart from the individual services and operational commands, all of which makes training and equipping for operations in cyberspace very bureaucratic and cumbersome. This is exacerbated by the overall defensive tone of the three mission sets: The DOD mainly defends their networks and provides defensive assistance to other agencies as required, a set of tasks that must be attended to every second of the day.

The DOD also performs offensive missions when directed to do so by the President. This is a very circumscribed set of missions, for several reasons. First, much as the entire U.S. Marine Corps would be swallowed by a megacity like Lagos, Nigeria, DOD offensive cyber assets would be overwhelmed by being everywhere and helping everyone. Additionally, many aspects of ongoing cyberspace activity do not pertain to the DOD at all. Just as most aviation activity does not concern the Air Force and most maritime activity does not involve the Navy, most cyber activity does not concern the Defense Department. An example would be an individual using PayPal to make a purchase from the web-retailer Amazon.

Operations in cyberspace as a military domain must therefore be a circumscribed mission set. Nevertheless, militarily relevant information, intelligence, criminal, and military-specific activities occur all over the Internet, so the military must be able to maneuver throughout all of cyberspace.

The Services and Cyber. The service chiefs provide cyber operations capabilities for deployment/support to Combatant Commands as directed by the Secretary of Defense.[47] In addition to joint strategy and doctrine, each service has its own doctrine to deal with cyber issues. This is not just because each service has its own history and culture. Cyber defense of ground forces is different from protecting platform-centric operations like those conducted by the Navy and Air Force. The Army must protect ground units, the Navy must protect groups of ships operating at sea across the globe, and the Air Force must protect individual flying platforms. At the same time, each service must protect its own infrastructure.

Therefore, under their Title 10 role as force providers to the combatant commanders, the services recruit, train, educate, and retain their own military cyber forces. There are four service component commands under U.S. Cyber Command (USCYBERCOM): U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, 24th Air Force, and U.S. Marine Corps Forces Cyber Command.[48] These service-specific units have several functions: They operate and defend their portion of the DODIN; perform full-spectrum cyber operations, meaning offensive and defensive; provide for cyber training and education; and undertake cyber research and capabilities development for their respective services.

Combatant Commands are responsible for geographic areas (such as European Command) or functional areas (such as Special Operations Command or U.S. Transportation Command) and provide operations instructions and command and control functions to the armed forces. They have a significant impact on how the service component cyber commands are organized, trained, and resourced—areas over which Congress has constitutional authority.[49] CCMDs share cyber information largely through USCYBERCOM and their own joint cyber centers, but various personnel also meet periodically to share information in collaboration sessions.[50]

USCYBERCOM was formed in 2010. It is a subunified command under U.S. Strategic Command (STRATCOM). Congress and the Obama and Trump Administrations have examined the propriety of dividing the two and promoting CYBERCOM to a full Combatant Command. This would allow CYBERCOM to work directly with other commands without having to work through an extra layer of command at STRATCOM. CYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified units and the DODIN. When so directed, it also prepares to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace and deny the same to adversaries,[51] and counter efforts by opponents to interfere with CCMD operations.

USCYBERCOM's main instrument of power is the Cyber National Mission Force, which conducts cyberspace operations to disrupt and deny adversary attacks against national critical infrastructure. It is the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. It planned to create 133 cyber mission teams by the end of fiscal year 2016;[52] the current plan is for all the teams to be fully functional by 2018.[53] The force eventually will consist of 13 National Mission Teams (NMTs), which are designed to defend the United States and its interests against cyberattacks of significant consequence; 68 Cyber Protection Teams (CPTs), which defend priority DOD networks and systems against priority threats; 27 Combat Mission Teams (CMTs), which aid Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations; and 25 Cyber Support Teams (CSTs), which provide analytic and planning support to the National Mission and Combat Mission teams.[54]

Put another way, National Mission Teams perform strategic operations, and CMTs conduct cyberspace operations in support of CCMDs. CPTs protect the DODIN, the services, and the CCMDs. CSTs support NMTs and CMTs.

This number of teams and their organizational distribution together ensure that the U.S. military meets the need to conduct offensive and defensive cyber operations around the clock in multiple commands and in multiple areas around the world, something quite unlike conventional military forces outside of active combat engagements. Once the Cyber Mission Force is fully established in 2018, the DOD no doubt will reassess its requirements and modify the force as needed based on experience.

Conclusion

The United States is challenged by a wide variety of state and non-state actors in cyberspace, which is already huge and constantly growing. Additionally, the U.S. has certain societal vulnerabilities at home that make facing these challenges more difficult. The Department of Defense, Department of Homeland Security, and Department of Justice have to operate in this environment as the U.S. government's three principal actors, which also seek partnerships with the private sector that operates almost all of the Internet.

The U.S. government seeks to protect the United States through protection and deterrence. Because of the size and complexity of cyberspace as well as domestic legal and cultural constructs in the United States, the DOD must circumscribe the scope of its operations in cyberspace, operating in the military cyber domain as required in the criminal, informational, intelligence, and operational fields. The DOD must defend itself, assist the President in other areas when directed to do so, and conduct defensive and offensive cyber operations as an integrated part of normal military operations.

In order to conduct these operations, the department has organized cyber forces in each of the services under the command of the Commander, United States Cyber Command, who has the task of training, educating, and building a world-class cyber force while simultaneously conducting cyber operations 24 hours a day around the globe. Conceptually, the DOD has recognized cyber as a domain, making it equal to sea, air, land, and space. "Cyber" promises to provide significant gains in the efficiency and effectiveness of U.S. military units through the full integration of conventional operations, cyber capabilities, and operations in the information environment.

Although military leaders understand the importance of cyber and information, not all understand the scope of the opportunities and challenges that cyber provides. The military services will have to expend more resources on training and equipping not only cyber forces, but all forces that will be serving in an environment where they are under continuous cyber-attack. Defensive cyber operations will protect forces from cyber-attacks while offensive cyber operations enable other conventional and special operations as an integrated whole. The U.S. is ahead of almost all other states in cyber capability, but it must continue to invest time and effort in order to maintain that lead.

Endnotes

1. Author’s interview with Brigadier General Greg Touhill, U.S. Air Force (Ret.), March 27, 2015.

2. See *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, May 2011, p. 8, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed July 5, 2017). Emphasis in original. Until the Trump Administration develops strategies, we must rely on Obama-era documentation.

3. The Merriam-Webster Dictionary defines wetware as “the human brain or a human being considered especially with respect to human logical and computational capabilities.” See “wetware,” Merriam-Webster.com, https://www.merriam-webster.com/dictionary/wetware (accessed August 14, 2017).

4. Internet World Stats, “Usage and Population Statistics: World Internet Users and 2017 Population Stats,” March 31, 2017–Update, http://www.internetworldstats.com/stats.htm (accessed August 14, 2017).

5. Steve Morgan, “Cyber Crime Costs Projected to Reach $2 Trillion by 2019,” *Forbes*, January 17, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3f772b113a91 (accessed June 26, 2017).

6. Among the most recent laws is the Cybersecurity Information Sharing Act of 2015, incorporated into the Consolidated Appropriations Act of 2016, Public Law 114-113, 114th Cong., which was signed into law by President Barack Obama on December 18, 2015. See Brad S. Karp, “Federal Guidance on the Cybersecurity Information Sharing Act of 2015,” Harvard Law School Forum on Corporate Governance and Financial Regulation, March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ (accessed July 5, 2017). Policies include a variety of executive orders, and important strategies include the May 2011 White House *International Strategy for Cyberspace* (see note 2, *supra*) and U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed July 5, 2017).

7. Joanna Belbey, “The Weakest Link in Cybersecurity,” *Forbes*, February 27, 2015, http://www.forbes.com/sites/joannabelbey/2015/02/27/the-weakest-link-in-cybersecurity/#38c0d3377410 (accessed June 26, 2017).

8. Brigadier General Jon T. Thomas, Deputy Director, Future Joint Force Development, Joint Staff, J7, “Joint Force Development: Moving from Concept to Reality,” 2013, p. 10, http://www.dtic.mil/ndia/2013/expwar/WThomas.pdf (accessed July 11, 2017); “Q&A with Rear Adm. Kevin Scott,” *CHIPS Magazine*, October–December 2015, http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=6918 (accessed July 11, 2017); and U.S. Department of Defense, *Department of Defense Fiscal Year (FY) 2017 President’s Budget Submission*, The Joint Staff, *Defense-Wide Justification Book Volume 5 of 5, Research, Development, Test & Evaluation, Defense-Wide*, February 2016, pp. 75–77, http://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2017/budget_justification/pdfs/03_RDT_and_E/RDTE_MasterJustificationBook_Joint_Staff_PB_2017.pdf (accessed July 1, 2017).

9. Eleven out of 47 systems were operating without a valid cyber-certificate authorization. See Evan Perez and Tom LoBianco, “OPM Inspector General Questioned Over Hacking Report,” CNN, updated June 17, 2015, http://www.cnn.com/2015/06/16/politics/opm-hack-ig-testimony/index.html (accessed June 26, 2017).

10. Ellen Nakashima, “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,” *The Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say (accessed June 26, 2017).

11. Kaspersky Lab, “Top 10 Tips for Educating Employees About Cybersecurity,” 2015, http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf?mkt_tok=3RkMMJWWfF9wsRonuKXNcO%2FhmjTEU5z16OglWa%2BzlMI%2F0ER3fOvrPUfGjI4ITMZjI%2BSLDwEYGJlv6SgFQrDHMalq1LgPXxE%3D (accessed July 5, 2017).

12. News release, “McAfee Labs Report Highlights Success of Phishing Attacks with 80 Percent of Business Users Unable to Detect Scams,” McAfee, September 4, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx (accessed June 26, 2017).

13. Susan Richardson, “Leaky End Users Star in DBIR 2016,” Data on the Edge, May 23, 2016, http://blog.code42.com/leaky-end-users-star-in-dbir-2016/ (accessed June 26, 2017).

14. Computer Emergency Response Team, “CERT Insider Threat Center,” Carnegie Mellon University, Software Engineering Institute, 2017, http://www.cert.org/insider-threat/cert-insider-threat-center.cfm (accessed June 26, 2017).

15. News release, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed July 5, 2017).

16. Kevin McCaney, “Report: US Suspects Russia in ‘Most Sophisticated’ Joint Staff Hack,” Defense Systems, August 6, 2015, https://defensesystems.com/articles/2015/08/06/joint-staff-email-hack-most-sophisticated.aspx (accessed June 26, 2017).

17. Dominic Rushe, "OPM Hack: China Blamed for Massive Breach of US Government Data," *The Guardian*, June 5, 2015, https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances (accessed June 26, 2017).

18. News release, "Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security," U.S. Department of Homeland Security, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (accessed June 26, 2017).

19. Anthony Cuthbertson, "Russian Cyber Attacks Aim to 'Destabilize' the West and NATO," *Newsweek*, February 3, 2017, http://www.newsweek.com/russian-cyber-attacks-hacking-nato-fallon-putin-destabilize-west-552050 (accessed June 26, 2017).

20. Ellen Nakashima and Matt Zapotosky, "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam," *The Washington Post*, March 24, 2016, https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html?utm_term=.b0f47016466d (accessed June 26, 2017).

21. Reuters, "North Korean Hackers Were Behind a Recent Major Cyber Attack," *Fortune*, March 15, 2017, http://fortune.com/2017/03/15/north-korea-hackers-cyber-attack/ (accessed June 26, 2017), and Sean Lyngaas, "North Korean Hackers Steal F-15 Design," *FCW: The Business of Federal Technology*, June 13, 2016, https://fcw.com/articles/2016/06/13/north-korea-f15-lyngaas.aspx (accessed June 26, 2017).

22. Timothy Maurer, "Cyber Proxies and the Crisis in Ukraine," Chapter 9 in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Talinn, Estonia: NATO CCD COE Publications, 2015), pp. 79–86, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf (accessed June 26, 2017).

23. Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019."

24. G. Alexander Crowther and Shaheen Ghori, "Detangling the Web: A Screenshot of U.S. Government Cyber Activity," *Joint Force Quarterly*, Issue 78 (3rd Quarter 2015), pp. 75–83, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-78/jfq-78.pdf (accessed June 26, 2017).

25. Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, Issue 75 (4th Quarter 2014), pp. 43–52, http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577560/jfq-75-the-limits-of-cyberspace-deterrence/ (accessed June 26, 2017); Gerry Smith, "Stuxnet: U.S. Can Launch Cyberattacks But Not Defend Against Them, Experts Say," *Huffington Post*, June 1, 2012, http://www.huffingtonpost.com/2012/06/01/stuxnet-us-cyberattack_n_1562983.html (accessed June 26, 2017); and Jared Serbu, "Foreign Cyber Weapons 'Far Exceed' US Ability to Defend Critical Infrastructure, Defense Panel Says," Federal News Radio, March 7, 2017, https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber-weapons-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel-says/ (accessed July 6, 2017).

26. This is not unique to cyber operations; it pertains to all such actions in all domains. An air strike intended to do one thing may generate a response that no one anticipated.

27. "Cyberspace," in U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, June 2017, p. 60, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed July 6, 2017).

28. David Aucsmith, "Cyberspace Is a Domain of War," War in Cyberspace, May 26, 2012, https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/ (accessed July 6, 2017). For another point of view, see Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, Issue 2 (2012), pp. 321–336, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf (accessed June 26, 2017).

29. Military operations as used here include military or paramilitary operations that other security forces (such as the Italian Carabinieri) or intelligence forces (such as the CIA) could perform but are mainly military in nature.

30. Manoj Kumar, "Indian Navy Raises Army for Cyber Front: Recruiting Cadets Against Chinese Hackers," *International Business Times*, July 13, 2012, http://www.ibtimes.co.in/indian-navy-raises-army-for-cyber-front-recruiting-cadets-against-chinese-hackers-362686 (accessed June 26, 2017).

31. Wesley Fenlon, "How Does ATM Skimming Work?" HowStuffWorks, November 8, 2010, http://money.howstuffworks.com/atm-skimming.htm (accessed July 6, 2017).

32. Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired*, May 17, 2016, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/ (accessed June 26, 2017).

33. Spencer Ackerman and Sam Thielman, "US Officially Accuses Russia of Hacking DNC and Interfering with Election," *The Guardian*, October 8, 2016, https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election (accessed June 26, 2017).

34. Tom Hamburger and Karen Tumulty, "WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations," *The Washington Post,* July 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.c84944ed0527 (accessed June 26, 2017).

35. Andreas Hagen, "The Russo–Georgian War 2008: The Role of the Cyber Attacks in the Conflict," AFCEA Cyber Conflict Case Studies Essay Contest, Second Place Entry, May 24, 2012, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf (accessed June 26, 2017).

36. Angel Rabasa, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, and Ashley J. Tellis, *The Lessons of Mumbai*, RAND Corporation, 2009, http://www.rand.org/pubs/occasional_papers/OP249.html (accessed July 6, 2017).

37. Colin Clark, "Carter Details Cyber, Intel Strikes Against Daesh at NORTHCOM Ceremony," *Breaking Defense*, May 13, 2016, http://breakingdefense.com/2016/05/carter-details-cyber-intel-strikes-against-daesh-at-northcom-ceremony/ (accessed June 26, 2017).

38. U.S. Department of Defense, Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, July 16, 2014, p. I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf (accessed June 26, 2017).

39. U.S. Department of Defense, "Fact Sheet: DoD Cyber Crime Center (DC3)," http://www.dc3.mil/ (accessed July 6, 2017).

40. Nakashima and Zapotosky, "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam."

41. Paul Thompson, "Semantic Hacking and Intelligence and Security Informatics," Conference Paper, International Conference on Intelligence and Security Informatics, Institute for Security Technology Studies, Dartmouth College, May 27, 2003, https://link.springer.com/chapter/10.1007/3-540-44853-5_40 (accessed June 26, 2017).

42. U.S. Department of Defense, Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R), February 5, 2013, p. II-5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed June 26, 2017).

43. Australian Government, Department of Defence, Australian Signals Directorate, "Strategies to Mitigate Cyber Security Incidents," February 2017, https://www.asd.gov.au/infosec/mitigationstrategies.htm (accessed July 5, 2017).

44. U.S. Department of Defense, *The DoD Cyber Strategy*, p. 3. Emphasis in original.

45. U.S. Department of Defense, "DOD 101: Overview of the Department of Defense," https://www.defense.gov/About/DoD-101/ (accessed June 26, 2017).

46. "The Defense Department procurement process can be confusing and complicated. There are a variety of contract types—each with its own pluses and minuses. The regulations can be daunting since they seem to be the size of the tax code. The competition for contracts can be fierce. There is a lot of paperwork." Michael Bame, "Overview of the DoD Procurement Process," ThoughtCo., updated August 10, 2016, https://www.thoughtco.com/overview-dod-procurement-process-1052245 (accessed June 26, 2017).

47. U.S. Department of Defense, Joint Chiefs of Staff, *Cyberspace Operations*, p. ix.

48. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed July 5, 2017).

49. Andrew Feickert, "The Unified Command Plan and Combatant Commanders: Background and Issues for Congress," Congressional Research Service *Report for Congress*, January 3, 2013, http://fas.org/sgp/crs/natsec/R42077.pdf (accessed July 5, 2017).

50. Rita Boland, "Command's Cybersecurity Crosses Domains, Directorates," *Signal*, June 1, 2013, www.acyberstrategufcea.org/content/?q=command%E2%80%99s-cybersecurity%E2%80%A8-crosses-domains-directorates (accessed June 26, 2017).

51. U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM)," September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed June 26, 2017).

52. Crowther and Ghori, "Detangling the Web."

53. U.S. Department of Defense, *The DoD Cyber Strategy*.

54. Ibid.