© Rodolfo Clix/Dreamstime.com

PART THREE

The Future of Cyberwarfare

CHAPTER 14 Cyberwarfare and Military Doctrine 317

CHAPTER 15 Pandora's Box: The Future of Cyberwarfare 333

© Rodolfo Clix/Dreamstime.com

Cyberwarfare and Military Doctrine

CHAPTER 14

OVER THE CENTURIES, MILITARY PLANNERS and strategists have developed a comprehensive body of knowledge regarding the conduct of warfare. This knowledge is known as military *doctrine*. The Chinese general Sun Tzu wrote one of the earliest known treatises on military doctrine, *The Art of War*, sometime around 500 BC. In it, he outlined basic strategies that every military commander should follow. In the book, he described the importance of developing plans, the use of deception as a key component of warfare, methods for exploiting an enemy's weak points, maneuvering and marching with an army, the effects of terrain on an army, and many other essential topics.

Of course, doctrine has evolved substantially in the time since Sun Tzu created his seminal work. Although *The Art of War* is still heavily cited today, modern military planners now have millennia of experience to draw upon. After Sun Tzu's work helped planners better understand the enemy, a German general, Carl von Clausewitz, changed the way planners understand the impact of terrain on warfare. The U.S. military, through the office of the Joint Chiefs of Staff, maintains a large set of doctrine publications that provide guidance to commanders in all of the military services. These publications are supplemented by service-specific doctrine documents that provide additional detail.

In the days of Sun Tzu, the military consisted of little more than soldiers on foot and on horseback along with rudimentary naval ships. The Chinese general could never have dreamed of tanks, destroyers, or fighter jets. Modern doctrine takes these advances into account, drawing upon the ancient sources but supplementing them with more recent knowledge about battlefield advances. Every time a military engages the enemy, planners learn more and incorporate this new knowledge into revisions of the doctrine to guide future commanders.

Cyberwarfare presents yet another frontier, one that is new to military commanders—just as the exploitation of the air and space domains was new to commanders in the world wars. Cyberwarfare doctrine is a rapidly evolving field, and there are relatively few publications in existence. The core document on the subject, *Joint Publication 3-12, Joint Cyberspace Operations*, remains classified and unavailable to nonmilitary cyberwarfare students.

Chapter 14 Topics

This chapter covers the following topics and concepts:

- What military doctrine is
- How the U.S. military is organized for cyber operations
- What the five pillars of cyberwarfare are

Chapter 14 Goals

When you complete this chapter, you will be able to:

- Describe the role and purpose of military doctrine
- Identify the major documents covering cyberwarfare doctrine
- Explain how the U.S. military is organized for cyber operations
- Explain the major concepts that must be addressed in cyberwarfare doctrine
- Describe the five pillars of cyberwarfare

Military Doctrine

In the words of General George H. Decker, who served as army chief of staff from 1960 until 1962, "Doctrine provides a military organization with a common philosophy, a common language, a common purpose, and a unity of effort." **Doctrine** provides commanders with a way to share thousands of years of accumulated military knowledge with their fellow officers in a consolidated format. Doctrine describes the manner in which a military will operate and provides commanders with guidance and advice on issues of strategic, operational, and tactical importance.

Doctrine is only advice, however. It provides a general philosophy for military operations, but it does not provide all of the answers. It remains the role of the military commander to read, understand, interpret, and apply doctrine in the unique circumstances of a particular battle, campaign, or war. In their *Compendium of Key Joint Doctrine Publications*, the Joint Chiefs of Staff sum up this important concept with a simple, catch phrase: "Doctrine Guides, Commanders Decide!"

In the Army's *Unified Land Operations* doctrine, the authors elaborate on this concept of a commander's discretion by stating:

> Doctrine is also a statement of how the Army intends to fight. In this sense, doctrine often describes an idealized situation and then contrasts the ideal with the reality Army leaders can expect. Doctrine provides a means of conceptualizing campaigns and operations, as well as a detailed understanding of conditions, frictions, and uncertainties that make achieving the ideal difficult. Doctrine also helps potential partners understand how the Army will operate. It establishes a common frame of reference and a common cultural perspective to solving military problems, including useful intellectual tools.

In the remainder of this section, you will learn some of the fundamental points of military doctrine accumulated over the centuries. These include the nine principles of war, the forms of warfare, and the levels of warfare.

Principles of War

According to U.S. military doctrine, **war** is "socially sanctioned violence to achieve a political purpose." The U.S. military believes that the effective execution of military operations relies upon nine core principles of war. These principles, as articulated in *Army Field Manual 3-0: Operations*, are:

- **Objective**—Every military action must have a clearly defined purpose. The **objective** of an operation should be both decisive and attainable. Commanders must clearly understand what they are attempting to achieve in a military action and use that knowledge to guide their decisions and instructions to subordinate commanders. The existence of a clear objective ensures that operations at lower levels are consistent with the higher-level commander's intent.

- **Offensive**—Military commanders must seize, retain, and exploit the initiative. By using the principle of **offensive**, they may dictate the nature, tempo, and scope of operations. By seizing the initiative, a military may compel its opponent to react. This provides the attacking force with greater freedom of action and increases the likelihood of successfully achieving its objective.
- **Mass**—Military commanders should concentrate their combat forces at the decisive time and location. This may take place in two ways. Commanders may choose to **mass** their forces *in time* by simultaneously striking multiple significant targets. Alternatively, commanders may opt to mass their forces *in location* by bringing overwhelming force against a single location. Each of these tactics may overwhelm the adversary and lead to victory.
- **Economy of Force**—Commanders should use the minimum amount of force necessary to achieve secondary objectives. Using **economy of force** allows commanders to achieve the principle of mass by allocating all remaining forces to achieving the primary objective.
- **Maneuver**—Applying power in a flexible manner keeps the adversary off guard. When performed effectively, **maneuver** keeps enemy troops at a disadvantage by forcing them to deal with new problems and dangers faster than they can react to the changing dynamics of the battlefield.
- **Unity of Command**—A single commander should be responsible for achieving each military objective under the principle of **unity of command**. In many cases, the nature of joint and multinational operations does not permit the assignment of a single commander. In those situations, multiple commanders must cooperate, negotiate, and build consensus.
- **Security**—Commanders must never allow enemy forces to gain an advantage. This is essential to preserving and protecting a military's power. **Security** may be bolstered by deception and results from defensive efforts against surprise, sabotage, interference, and intelligence operations conducted by the enemy.
- **Surprise**—When attacking, military forces should strike the enemy at an unexpected time or place. **Surprise** brings shock value by surprising an enemy and offering attackers a temporary battlefield advantage. Surprise does not require a completely unaware enemy—it only requires that the attack take place in a time or place where the enemy can't immediately react in an effective manner.
- **Simplicity**—Military plans should be simple, clear, and concise. The more complex or ambiguous a set of orders, the more likely it is that the unit will fail to achieve its objective. **Simplicity** reduces confusion and misunderstanding.

The principles of war are not consistent from nation to nation. Every country's doctrine embodies a similar set of principles, but there are often additions, modifications, and deletions. For example, the British Defense Doctrine outlines 10 principles of warfare: Selection and Maintenance of the Aim, Maintenance of Morale, Offensive Action, Security, Surprise, Concentration of Force, Economy of Effort, Flexibility, Cooperation, and Sustainability.

In fact, the principles of war are not even consistent among military forces of the same nation. Although the U.S. Army embraces the nine principles outlined above, the Joint Chiefs of Staff use a different list, known as the *Principles of Joint Operations*. The 12 principles in that document include the 9 Army principles, along with 3 additional items:

NOTE

After the 1984 passage of the Goldwater-Nichols Act, responsibilities for U.S. military operations were divided between the individual military services and joint commands. Services are responsible for training and equipping troops, whereas joint commands fight wars through combatant commanders.

- **Perseverance**—Military commanders must take measures to ensure that the commitment exists to achieve the desired end state. Some military operations may take years to achieve their desired objectives. When using the principle of **perseverance**, commanders must be patient, resolute, and persistent when employing their forces in support of long-term objectives.
- **Legitimacy**—Military operations must take place within the confines of appropriate authority. The actions of military commanders must have **legitimacy**, or be consistent with national laws as well as international treaties and obligations. Commanders have a particular obligation to ensure that the actions of units and individuals are consistent with the Law of Armed Conflict.
- **Restraint**—While conducting military operations, commanders should use **restraint**, or limit collateral damage and prevent the unnecessary use of force. Military forces must be careful and disciplined. The unrestrained use of force may violate the law and antagonize both friendly and neutral parties, damaging the legitimacy of a military action.

These principles of warfare and joint operations form the core of military doctrine. Although different nations and military services may interpret and articulate them differently, they are generally respected as fundamental truths. Many of the principles date back thousands of years, appearing even in Sun Tzu's *The Art of War*. For example, Sun Tzu described the modern principles of Offensive and Security when he stated, "The clever combatant imposes his will on the enemy, but does not allow the enemy's will to be imposed on him."

TIP

Students trying to remember the principles of warfare often rearrange them to form the acronyms MOSS MOUSE or MOOSE MUSS to help them remember the first letter of each principle.

Forms of Warfare

As military strategists think about war, they organize it into two general forms: traditional warfare and irregular warfare. These are not neat subdivisions but rather broad generalizations that allow planners to discuss the different forms of warfare using a common context and language. They define the two primary forms of warfare in these ways:

- **Traditional warfare** includes large-scale conflict between nations or groups of nations. U.S. military doctrine defines traditional warfare as "characterized as a violent struggle for domination between nation-states or coalitions and alliances of nation-states. This form is labeled as traditional because it has been the preeminent form of warfare in the West since the Peace of Westphalia (1648) that reserved for the nation-state alone a monopoly on the legitimate use of force." Nations engage in traditional warfare for the purpose of imposing their will on other nations or preventing other nations from doing the same to them.
- **Irregular warfare** can be just as violent as traditional warfare but is marked by several differences. In U.S. military doctrine, irregular warfare is defined as "characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)." Notice two important differences in this definition. First, the participants in irregular warfare may include nonstate actors. Second, the purpose is not the imposition of wills between nations but the quest for legitimacy and purpose over a population.

FYI

Although U.S. military doctrine divides warfare into the traditional and irregular forms, not all military historians and strategists agree with this approach. Other common schemes for dividing warfare into two categories include:

- Regular versus irregular warfare
- Traditional versus nontraditional warfare
- Traditional versus untraditional warfare
- Conventional versus unconventional warfare

The military settled on the traditional versus irregular language as its standard. The term *conventional* warfare was discarded because it was widely used during the cold war to refer to non-nuclear warfare. Doctrine developers thought that the previous widespread use of the term for another purpose would cause confusion.

It is important to note that nation-states may engage in both traditional and irregular warfare and, in fact, the military engagements of the United States since September 11, 2001, have been primarily irregular in nature. The U.S. military presence in Iraq and Afghanistan during this century has focused extensively on influencing the populations of those countries and encouraging them to adopt democratic forms of government favorable to U.S. interests. The military has also been heavily engaged in the "war on terrorism," which has clearly been a national priority. It does not meet the definition of traditional warfare because the adversary is not a nation-state.

Cyberwarfare can fit within either of these forms of warfare. Nations may engage in cyberwarfare operations against each other as a component of traditional warfare. At the same time, nations may use cyberwarfare operations against nonstate actors, and nonstate actors may use cyberwarfare against nation-states when engaging in irregular warfare.

NOTE

The field of battle is complex and full of uncertainty and chance. Military scholar and general Carl von Clausewitz described this confusion as "the fog of war."

Levels of Warfare

The *forms* of warfare distinguish between warfare actions based on both the types of adversaries engaged in the war and their strategic objectives. At the same time, military commanders achieve these objectives by engaging in actions at different *levels* of warfare. These levels, the strategic level, operational level, and tactical level, are used to set loose boundaries around warfare at the appropriate echelons of command authority.

The **strategic level** of warfare addresses the national-level objectives of the war. It includes very broad goals, including both the national policy issues at stake and the strategies used to engage the enemy across an entire theater of operations. In the United States, strategic-level objectives are set by senior political and military officials, including the president, secretary of defense, and commander of the Joint Chiefs of Staff.

The lowest level of warfare is the **tactical level**. Tactical activities include the specific use of military units that engage each other in battles and small-unit actions. Commanders at this level must be concerned with the "nuts and bolts" of warfare. They direct the movements of individual units, personnel, and weapons systems. Military engagements at the tactical level are typically short term in duration and have extremely specific objectives. "Take that hill!" is an example of a tactical military objective.

In between the strategic and tactical levels lies the **operational level** of warfare. At this level, commanders set the objectives for military campaigns and major operations. These objectives link together the national policies set by senior

Cyberattack Strikes the Air Force

In the Air Force's *Cyberspace Operations* doctrine document, the authors cite an example of a real-world cyberattack against the Air Force's assignment management system. This excerpt from the Air Force Office of Special Investigations briefing on the incident describes the risk of cyberattacks against military information systems:

> In May [20]05, an unknown subject obtained unauthorized user level access to the Assignments Management System (AMS). Using that access, the subject was able to view information contained within the AMS, but was unable to alter information or gain access to any other Air Force computer systems. Computer records indicate that the subject gained access to AMS via a senior Air Force official's account. The compromised AMS account was set with privileges which allow the user to review any active duty Air Force member's single unit retrieval format (SURF) data from anywhere in the world with an Internet connection. SURF records contain sensitive data, such as assignment history, security clearance, personal identification information, rank, position, and duty status. The subject gained access to the web based account using the "forgot password" function to answer the challenge questions required to change the account password. The challenge questions asked for biographical information on the senior official, which was readily available on the Internet.
>
> Upon review, it was determined that the senior USAF official's account had been used to view the SURF records of 37,069 Air Force members. Log analysis indicates the intrusion initially originated from forty-one different source IP addresses throughout the duration that the compromised account was used by the subject.
>
> Throughout this duration, the subject's activity originated from approximately twelve additional US based Internet Protocol (IP) addresses, which were later determined to be open proxies that the subject used to mask their true place of origin. There were no foreign-based IP addresses used after the incident was reported. Court order subpoenas were served on all US-based source IP addresses from which the compromised AMS account was accessed; fifty in total. Information obtained via court order subpoenas identified the last known point of the origin. However, local law enforcement indicated that the information required to further identify the subject was no longer available.

The scope and duration of this attack against a sensitive military computer system reflect the sophistication and selective targeting used by adversaries engaged in cyberwarfare.

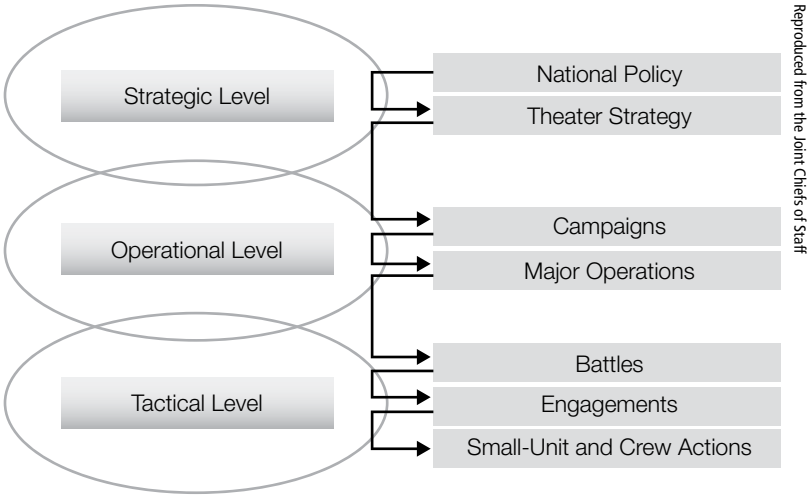


FIGURE 14-1
The levels of warfare: strategic, operational, and tactical, as described in U.S. military doctrine.

leaders with the movements of military units at the tactical level. When referring to this level of warfare, U.S. military doctrine refers to the term *operational art* as follows:

> The focus at this level is on the planning and execution of operations using operational art: the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means.

Figure 14-1 illustrates the relationship between the various levels of warfare. Note that the boundary lines drawn between them overlap. The lines between actions at the strategic and operational levels are blurred, as are the lines between operational and tactical activities.

As with the forms of warfare, cyberwarfare operations may take place at any of these levels of warfare. At the strategic level, cyberwarfare may include intelligence activities that provide critical information to senior government officials as they set national policies. At the operational level, a military campaign might include a significant cyberwarfare component that disables critical enemy defense systems just before friendly forces launch a massive offensive strike. Finally, at the tactical level, commanders might engage in cyberwarfare activities designed to support individual units on the ground as they engage the enemy in a battle.

Organizing for Cyber Operations

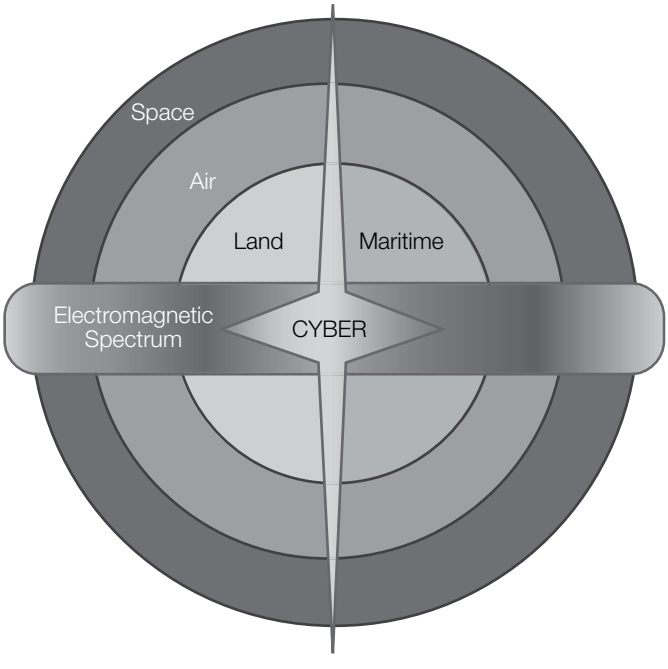
Military forces around the world typically organize themselves based upon the types of operations in which they engage. For example, consider the military organization of the United States, which consists of four primary components:

- The U.S. Army is primarily engaged in operations covering the land domain of warfare.
- The U.S. Navy is primarily engaged in operations covering the sea domain of warfare.
- The U.S. Marine Corps is engaged in operations that cross between the land and sea domains of warfare.
- The U.S. Air Force is concerned with both the air and space domains of warfare.

There is, however, no "U.S. Cyber Force" that bears primary responsibility for the cyber domain of warfare. Cyberwarfare responsibility is widely distributed among military units, with sometimes confusing and overlapping lines of authority. In addition, military and nonmilitary agencies that fall outside the armed services also participate in cyberwarfare operations. For example, the U.S. National Security Agency (NSA) is a component of the Department of Defense that is led by a military flag officer but is also somewhat independent of the traditional military command structure. Figure 14-2 illustrates the overlapping relationship between cyberwarfare and the traditional domains of warfare.

FIGURE 14-2

The cyber domain of warfare functions across all of the traditional domains of warfare.



Reproduced from Air War College, Air University

FYI

The DoD released a new joint publication, *JP 3-12: Joint Cyberspace Operations* in February 2014. In its *Compendium of Key Joint Doctrine Publications*, the Joint Chiefs claim that JP 3-12 does "address the uniqueness of military operations in cyberspace, clarify cyberspace operations-related command and operational interrelationships, and incorporate operational lessons learned." However, JP 3-12 itself is classified as Secret and is not available for public review.

How does the U.S. military organize for cyberwarfare? Each military unit has its own cyberwarfare component and the actions of these components are supposed to be coordinated by the U.S. Cyber Command (USCYBERCOM). In its mission statement, USCYBERCOM "plans, coordinates, integrates, synchronizes and conducts activities to direct the operations and defense of specified Department of Defense information networks and prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/allied freedom of action in cyberspace and deny the same to our adversaries."

That is a very confusing and unclear mission statement, and it is somewhat reflective of the confusion surrounding cyberwarfare activities in a military that is organized to fight in the traditional domains of warfare. In July 2011, the U.S. Government Accountability Office (GAO) performed an assessment of the Department of Defense's cyberwarfare efforts and found that they were severely deficient. In one of the findings, GAO identified a lack of consistent doctrine:

> Several joint doctrine publications address aspects of cyberspace operations, but DOD officials acknowledge that the discussions are insufficient; and no single joint publication completely addresses cyberspace operations. While at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention "cyberspace operations," none contained a sufficient discussion of cyberspace operations. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine. However, there is no timetable for completing the decision-making process or for updates to existing doctrine.

The second significant finding in GAO's assessment relates to the extremely complex and overlapping organizational responsibilities for cyberwarfare. Figure 14-3, taken from the GAO report, illustrates the complexity of the situation, with many components having multiple reporting relationships that do not meet until they reach the cabinet-level post of secretary of defense. In the words of the GAO:

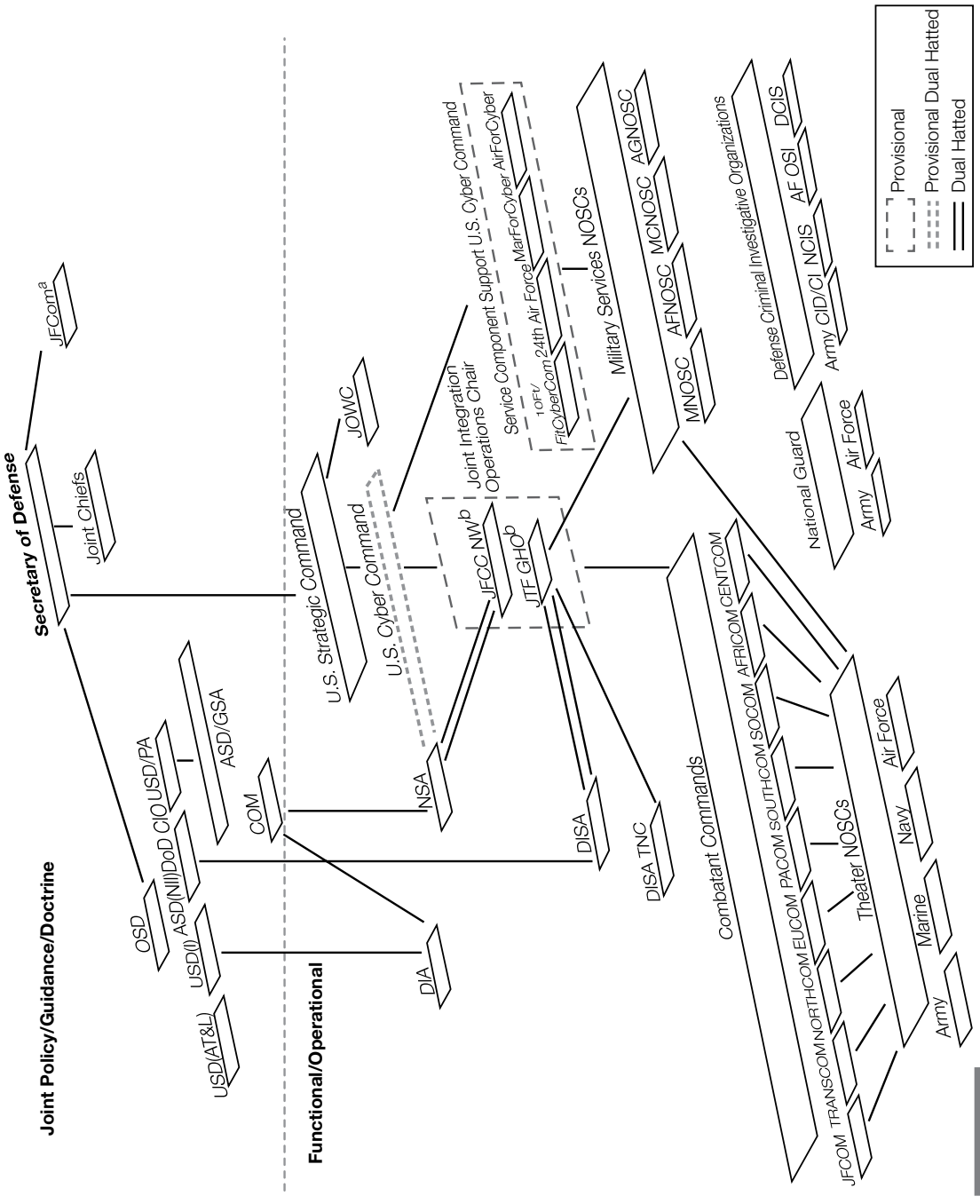


FIGURE 14-3
Organization chart of Department of Defense cyberoperations structure, as assessed by the Government Accountability Office in 2011.
Reproduced from GAO

> DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both its own command and a geographic combatant command. Without complete and clearly articulated guidance on command and control responsibilities that is well communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyberspace operations.

U.S. Strategic Command (USSTRATCOM)

As shown in Figure 14-3, one of the nexus points for command of cyberspace operations falls with the U.S. Strategic Command (USSTRATCOM). When it was formed during the cold war, USSTRATCOM was focused on defending the United States against the threat posed by the Soviet Union. In particular, USSTRATCOM had responsibility for the nation's nuclear forces.

With the end of the cold war, the mission of USSTRATCOM changed and broadened in scope. First, the command merged with the U.S. Space Command and assumed responsibility for military satellites and other space operations. Second, the command was chosen to take on the cyberwarfare mission for the U.S. military. The USSTRATCOM mission statement now reads, in part: "The missions of U.S. Strategic Command are to deter attacks on U.S. vital interests, to ensure U.S. freedom of action in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations."

U.S. Cyber Command (USCYBERCOM)

USSTRATCOM manages cyberspace operations through the use of a "subordinate unified command," the U.S. Cyber Command (USCYBERCOM). As a subordinate unified command, USCYBERCOM has full command authority over cyberspace operations, but reports through the commander of USSTRATCOM.

FYI

A careful examination of the USCYBERCOM emblem reveals that it contains the string "9ec4c12949a4f31474f299058ce2b22a" written in the circle between the name of the command and the inner logo. This is the MD5 hash of the command's mission statement.

The command is located at Fort Meade, Maryland, home to the NSA, and is led by a four-star flag officer. To date, two officers have held this position on a permanent basis. General Keith Alexander held the position from the command's creation in 2010 until his retirement in 2014. Admiral Michael Rogers assumed command in April 2014. Both officers held the command of USCYBERCOM concurrently with their service as director of the National Security Agency.

As a unified organization, USCYBERCOM is composed of military service components representing each of the uniformed services:

- Twenty-Fourth Air Force (Air Forces Cyber)
- Second Army (Army Cyber Command)
- Tenth Fleet (Fleet Cyber Command)
- Marine Corps Cyberspace Command

Each of these component commands has responsibility for cyberspace operations within its respective military service.

Five Pillars of Cyberwarfare

As the nation continues to chart its course in cyberspace, the Department of Defense has outlined a strategy for cyberspace operations that consists of five major pillars. These pillars are the strategic initiatives that the government considers essential to building and maintaining the nation's cyberwarfare superiority. Described in the *Department of Defense Strategy for Operating in Cyberspace*, the five pillars include:

- "Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."
- "Employ new defense operating concepts to protect DoD networks and systems."
- "Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy."
- "Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity."
- "Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation."

The ability of the United States, or any nation, to effectively engage in the new domain of cyberspace depends upon the successful fulfillment of these five strategic objectives.

Ten Things Every Airman Should Know

The Air Force continues to educate its officers and enlisted personnel about the effects that their personal actions can have on national security. General Norton A. Schwartz, former chief of staff of the Air Force, issued the following 10 cyber tips to airmen, entitled "Ten Things Every Airman Should Know":

1. The United States is vulnerable to cyberspace attacks by relentless adversaries attempting to infiltrate our networks at work and at home—millions of times a day, 24/7.
2. Our adversaries plant malicious code, worms, botnets, and hooks in common websites, software, and hardware such as thumbdrives, printers, etc.
3. Once implanted, this code begins to distort, destroy, and manipulate information, or "phone" it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.
4. The adversary attacks your computers at work and at home knowing you communicate with the Air Force network by email or by transferring information from one system to another.
5. As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates, and your country.
6. You significantly decrease our adversaries' access to our networks, critical Air Force information, and even your personal identity by taking simple action.
7. Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.
8. Do not connect any hardware or download any software, applications, music, or information onto our networks without approval.
9. Encrypt sensitive but unclassified and/or critical information. Ask your computer security administrator for more information.
10. Install the free Department of Defense anti-virus software on your home computer. Your computer security administrator can provide you with your free copy.

While these tips were issued by the Air Force, they apply equally to anyone engaged in cyberwarfare or who may be a target of cyberwarriors!

CHAPTER SUMMARY

Military doctrine provides commanders at all levels of the military with the guidance they need to understand the objectives and strategies of higher-level commanders. Doctrine provides a blueprint for those commanders as they seek to understand the strategic and operational environment. Commanders are then responsible for interpreting that environment and making decisions that are consistent with both battlefield realities and military doctrine.

As a new domain of warfare, cyberspace presents a challenge to military commanders, similar to the challenge they faced when adapting to the new air domain during the world wars. The current state of doctrine and organization surrounding cyberwarfare is somewhat confused. As pointed out in a GAO audit, there are many different doctrine documents that discuss cyberspace operations, offering sometimes-conflicting guidance. The military also has many different components; each seeks to address cyberwarfare issues but does so within a confusing and overlapping command structure. As the nation becomes more sophisticated in its cyberwarfare operations and capabilities, these issues must be resolved.

KEY CONCEPTS AND TERMS

Doctrine
Economy of force
Irregular warfare
Legitimacy
Maneuver
Mass
Objective
Offensive
Operational level
Perseverance
Restraint
Security
Simplicity
Strategic level
Surprise
Tactical level
Traditional warfare
Unity of command
War