PART ONE

The Cyberwarfare Landscape

CHAPTER 1

Information as a Military Asset

WHAT DO YOU THINK OF when you imagine military assets? Chances are that your thoughts immediately go to the traditional implements of armed conflict—tanks, naval ships, rifles, fighters, and bombers. These are, after all, the traditional, highly visible ways that armies engage each other on the battlefield. However, throughout the history of warfare, information has played a crucial role in shaping the ways that nations engage each other in warfare.

From the earliest wars waged between ancient forces to the complex maneuvering of today's tremendous military forces, military leaders have sought to use information as a weapon. They seek information about opposing forces and attempt to spread misinformation about their own plans and objectives in the hope of skewing the outcome of battles. Information is, and always has been, a critical military asset.

Over the past century, society has made dramatic improvements in the ways people store, process, and transmit information. During the Second World War, the few computers that were available to the military were highly complex devices that took up tremendous amounts of space and had primitive computing capacity. Today, it's hard to find someone who doesn't have a smartphone in his or her pocket that possesses literally millions of times the computing power of those "supercomputers."

It only makes sense that the advances in information technology (IT) that have changed the way people do business also change the way nations fight wars. The first natural extension of this technology is to perform the same tasks in the military sector that it performs in the private sector. After all, armies need human resources systems, spreadsheets, and electronic mail. It's easier to present an intelligence briefing using PowerPoint slides than transparencies on an overhead projector. Militaries can also use these technologies for military-specific purposes, such as maintaining target databases, calculating missile trajectories, and similar

tasks. Information is a powerful tool in warfare and information technology is a way to magnify the impact that superior information can have on the battlefield.

Once you understand information as a critical military asset, it is not a significant leap to imagine information as a military target. If an information system provides a military with a battlefield advantage, the opposing force would surely want to deny their enemy the use of that weapon. Actions they can take to destroy enemy information technology are, therefore, now high on the priority lists of modern military forces.

How do militaries attack the information infrastructure of their adversaries? It is certainly possible to engage them using traditional weapons. Dropping a bomb on a data center is a very effective way of destroying the computer systems it contains. But what if the enemy has a backup data center? In addition, sending a bomber to a data center deep within enemy territory puts friendly airmen in harm's way and requires an overt hostile action that may trigger an undesired escalation in the conflict between two nations.

This text explores the concept of *cyberwarfare*. This involves taking the information war to a new level—not only seeing information as a military asset and a potential target, but also using information technology as a potential weapon. Attacks that take place in the cyber domain use information technology resources to wage war against the technology infrastructure of an opposing force. This may include attacks designed to cripple enemy information systems but, as you will learn, may also include the use of electronic weapons to destroy traditional targets.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What cyberwarfare is
- How warfare has evolved over the course of history
- What the role of information in warfare is
- What role cyber plays in the domains of warfare
- What categories of information operations the cyber domain entails
- What the techniques of information operations include

Chapter 1 Goals

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

- Describe the relationship between cyberwarfare, information warfare, and information operations
- Explain the role that information has played in armed conflict over the course of military history
- Describe the concept of cyberwarfare and how it relates to the traditional domains of armed conflict
- Describe the techniques used to effectively fight in the cyber domain

What Is Cyberwarfare?

Cyberwarfare includes a wide range of activities that use information systems as weapons against an opposing force. The strategy outlined by the United States Director of National Intelligence (DNI) reflects the fact that the history of cyberwarfare is at a turning point. This domain of fighting is emerging and the actions that countries take over the next several decades will shape doctrine, tactics, techniques, and procedures for years to come.

NOTE

Although this text offers a concise definition of cyberwar, it is important to point out that there is no agreed-upon definition of cyberwar among military planners.

The DNI's threat assessment in this area, relied upon by U.S. government officials, considers the cyberthreat to be a major threat to national security over the coming years. The risks come from two major activities of cyberwar:

- **Cyberattacks** are nonkinetic, offensive operations that are intended to cause some form of physical or electronic damage. These cyberattacks are what most people envision when they hear the term *cyberwar*. Cyberattacks may range from a computer virus designed to disrupt the control systems of unmanned aerial vehicles (UAVs or *drones*) to stealthy invasions of an adversary's information systems to alter information used to make military decisions.
- **Cyberespionage** involves intrusions onto computer systems and networks designed to steal sensitive information that may be used for military, political, or economic gain. Cyberespionage is akin to traditional intelligence-gathering operations that seek to gain access to protected information.

Cyberwarfare is the combination of activities designed to participate in cyberattacks and cyberespionage, on either side of the attack. Militaries certainly seek to attack other forces and will use the weapons of cyberwarfare to gain advantage when possible.

At the same time, militaries must defend themselves against the cyberwarfare activities of other nations and nonstate actors. The combination of these offensive and defensive activities is cyberwarfare.

Likelihood of Cyberwar

Is cyberwarfare likely to occur? Military and technology experts around the world hotly debate this question. Although there is no broad agreement on this question, the most common thought, echoed by the U.S. government's threat assessment, is that large-scale catastrophic cyberattacks are unlikely in the short term. Very few groups possess the ability to wage sophisticated, sustained cyberwarfare. Outside of the governments of the United States, China, Israel, and Russia, there are only a handful of countries known to have significant cyberwarfare programs. It is unlikely that any of these nations would launch a significant cyberattack against an adversary unless it was part of a larger war that crossed traditional domains.

Although it may be unlikely that the world will see a massive cyberattack in the next few years, that does not mean that cyberwarfare won't take place. Remember, cyberwarfare has two major activities: cyberattack and cyberespionage. It is extremely likely that each of the nations just identified has extremely sophisticated cyberespionage capabilities and is currently using them against many different adversaries.

As an example, the U.S. National Security Agency (NSA) appeared in the global spotlight after a defense contractor, Edward Snowden, released caches of classified information that provided the world with a glimpse into the inner workings of an agency dedicated to cyberespionage activities. The Snowden documents revealed a massive worldwide electronic spying operation that caught billions of people in its dragnet. According to the documents, the NSA cooperated with technology companies to systematically undermine the security of products and collect information about system users and, when the companies would not cooperate, conducted cyberespionage operations to gain surreptitious access to those information systems.

It would be naïve to think that the United States is the only nation that sees the value of information that may be gained through cyberespionage. It is very likely that other technologically advanced nations have military units conducting similar activities designed to retrieve sensitive information from potential future adversaries and use it for military, political, and economic advantage. Cyberespionage is not only likely, it is happening on a large scale every day.

Finally, although it is unlikely that a nation will launch a massive cyberattack against another nation, it is very likely that cyberattacks will occur. Throughout this text, you will read examples of such attacks that have taken place over the past decade, and these examples will only continue to multiply. What, then, is the difference between these attacks and all-out cyberwarfare?

With limited exceptions, the cyberattacks that take place today are not traceable back to a national government. They are the work of **nonstate actors**: individuals or groups that seek to participate in cyberwarfare but do so independently, without the endorsement of a national government. These individuals and groups may be extremely motivated to conduct hostile actions to advance their agendas but lack the sophistication and technical capability to conduct a sustained cyberwar. They do, however, pose the threat of causing significant damage against a limited scope of targets.

Consider, as an example, the hacker group known as Anonymous. Founded in 2003, this loosely organized collective of activist hackers waged a collective cyberwar against organizations that it found distasteful. The targets of Anonymous have included the Church of Scientology, government agencies, financial institutions, and proponents of defending intellectual property. Using Internet message boards, the members of Anonymous vote to select targets of their attacks and then wage cyberwarfare against their victims. These types of attacks can have crippling effects on their targets, but organizations of this type simply do not possess the scale to wage a massive cyberwar against an organized opponent.

Cyberwarfare Terminology

The terminology of cyberwarfare is not agreed upon and may often seem confusing and overlapping. This text covers the major activities of cyberwarfare, including both offensive and defensive activities. Some would argue that defensive activities are not truly cyberwar, but the authors disagree and choose to include them. Students of cyberwar must understand both offensive and defensive capabilities, tactics, and procedures. They are inseparable.

Also, many people make the distinction between cyberwarfare and **information operations**, a broader term used to describe the many ways that information affects military operations. The military defines information operations as actions taken to affect an adversary's information and information systems while defending your own information and information systems.

Finally, the military services also talk about **information warfare** as information operations conducted during a time of crisis or conflict to achieve specific objectives.

What is commonly agreed upon is that cyberwarfare activities (including cyberattack and cyberespionage) are part of information operations and that information operations includes activities (such as psychological operations and military deception) that are not included in cyberwarfare. This text uses the terms *information operations* and *information warfare* interchangeably.

The Evolving Nature of War

In 1775, a ragtag colonial military consisting of American patriots engaged the British military, the strongest armed force in the world, in battles at the towns of Lexington and Concord in Massachusetts. The colonists had very little going for them. They were outgunned, ill trained, and unprepared for a major military assault. They fought a conventional military battle using the linear formations of the time and, despite the odds, they prevailed, sending the British into a retreat toward Boston. That's when things began to get interesting.

Rather than allowing the British to retreat, the colonists set up ambush positions along the route and began to fight a type of guerrilla warfare that the British army had never before seen. They hid in the woods, behind rocks, and in ditches and relentlessly attacked the retreating forces. British General Hugh Percy, sent to rescue the retreating forces, said "The rebels attacked us in a very scattered, irregular manner, but with perseverance and resolution, nor did they ever dare to form into any regular body. Indeed, they knew too well what was proper, to do so. Whoever looks upon them as an irregular mob, will find himself very much mistaken."

Fast-forward 235 years. In 2010, a nuclear enrichment facility located in Natanz, Iran, suffered critical technical problems that caused significant damages to centrifuges critical to the uranium-enrichment process. These technical issues were quickly linked to a computer worm known as Stuxnet that seemed specifically targeted at damaging the Natanz facility. Although no nation has officially claimed credit, both the United States and Israeli governments have openly hinted at their involvement in the attack.

What do these two military actions have in common? They both mark major turning points in the evolving history of warfare. Before the American Revolution, it was common (in Europe) to fight in the British style—opposing forces lined up facing each other and fired their weapons until one side either fell or retreated to safety. The use of ambush techniques took the British by surprise and contributed to the eventual American victory. Before Stuxnet, the use of computers as weapons was not a mainstream military tactic. The attack on Natanz marked a bridging of the world of cyberwarfare and conventional warfare. The world is now on notice that the weapons of cyberwar are sophisticated and can cause damage in the physical world, similar to that caused by conventional weapons.

The past two centuries have seen a gradual evolution of the way nations fight. The two world wars were highly conventional battles between massive forces, but they saw the introduction of the air domain in warfare. The Japanese surprise attack on Pearl Harbor ushered in American participation in World War II and eventually resulted in the unleashing of atomic weapons on Hiroshima and Nagasaki that ended the war. The introduction of nuclear weapons on the international stage changed the course of history, resulting in a 30-year cold war that was punctuated by conflicts that kept the world on edge—wondering if the theory of mutually assured destruction would prevent the United States and Soviet Union from "nuking each other into the stone age."

This type of evolution will continue over the centuries to come. Societies will continue to engage in armed conflict and will seek to incorporate new technologies on the battlefield. Some of these will enhance physical weapons, but there will be a continuing evolution in the world of cyberwarfare. New weapons and tactics will take the stage and new ways of fighting will change the future face of conflict between nations and nonstate actors.

The Role of Information in Armed Conflict

Throughout the history of armed conflict, militaries and military leaders have understood the importance of protecting sensitive information. They have also gone to great lengths to obtain the sensitive information of others that may be of strategic or tactical value. The development of cyberespionage techniques is a natural extension of this ancient objective. With large amounts of information stored in computer systems, it is only natural that militaries would seek to infiltrate those systems and gain access to enemy secrets.

Ancient Warfare

One of the earliest recorded attempts to preserve military secrets dates back to approximately 50 BC, when Julius Caesar faced a communications dilemma. As a military leader with forces spread throughout the reaches of the Roman Empire, Caesar needed to communicate with his generals on a regular basis to convey orders and status updates. Without access to any electronic means of communication, Caesar had to rely upon written documents, carried by messengers among his troops. Caesar's adversaries knew that these communications would be sent and would surely want to intercept anyone suspected of being a messenger in hopes of gaining access to Caesar's strategy.

Caesar compensated for this vulnerability in his communications system by using a simple, but effective technology known as the Caesar cipher. He simply went through messages character by character and shifted each character three places to the right. For example, every *A* in the message became a *D*. Every *B* became an *E*, every *C* became an *F*, and so on. He then sent this encoded message on its way with a messenger. Those who intercepted the message were not aware of the encoding system and, lacking knowledge of codes and ciphers, were unable to decipher its meaning.

When a general in the field received a message from Caesar, he knew how to reverse the encoding system: Simply shift each character three places to the left. Convert the *D*s back to *A*s, the *E*s to *B*s, the *F*s to *C*s, and so on; eventually the original message from Caesar would appear.

Although the Caesar cipher was rudimentary, it worked effectively, preserving the security of Caesar's communications system and opening an era of communications security in military operations. Modern militaries share the same objective of both protecting their own communications and intercepting the communications of their adversaries. The difference is only that the tools of information security and cyberespionage have become technologically sophisticated.

World Wars

About 2,000 years after Caesar, military forces continued to find themselves focused on finding methods to preserve the secrecy of communications. The technology used to transmit those communications improved dramatically with the invention of the radio. Unfortunately, the same technology that made it easier for friendly troops to communicate also made it possible for the enemy to intercept those communications. Radio waves travel freely through the air. Anyone with an antenna can intercept them.

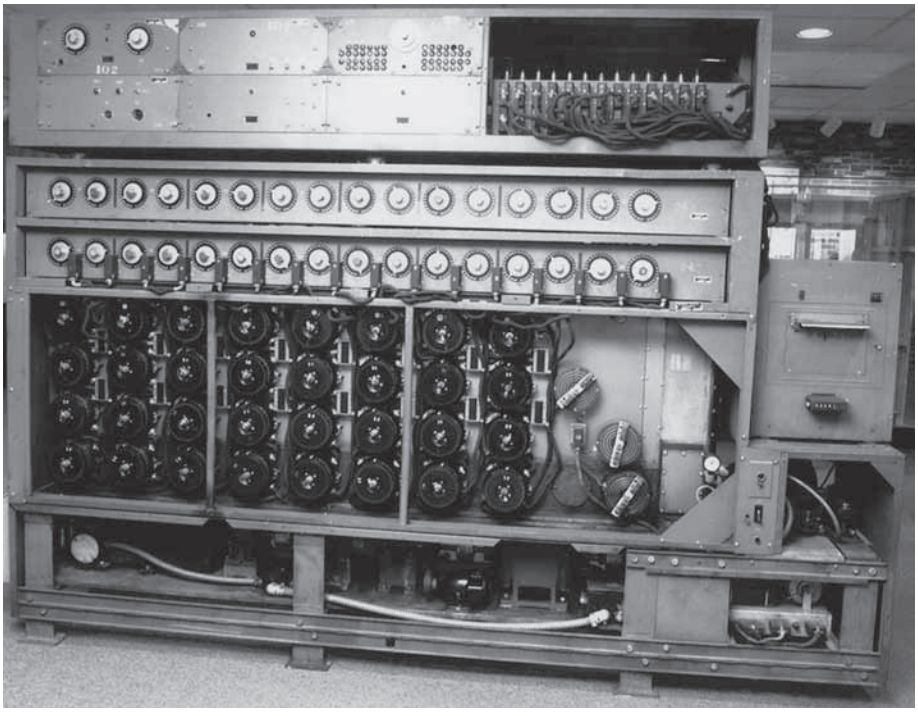
The wide use of radios made the use of codes more important. The Caesar cipher got the job done for the Roman army, but it was too simple for modern use. Anyone with a basic knowledge of codes could easily decipher this simple cipher. Specialized mathematicians, known as *cryptographers*, worked hard to develop encryption technology that made it hard for the enemy to decipher communications.

During World War II, the German and Japanese governments developed a specialized encryption device known as Enigma. This system, shown in Figure 1-1, resembles a typewriter. The operator first sets the machine to the code of the day. He then would key in the message letter by letter. As he pressed each key, a different letter would light up on the device. This would be the letter transmitted as part of the encrypted message. When the receiver got the message, he would reverse the process by pressing the keys corresponding to the letters in the encrypted message. The letters of the original message would then light up on the Enigma device.

U.S. Government Photo

FIGURE 1-1

One of the Enigma machines captured by the Allies during World War II on display at the National Security Agency's National Cryptologic Museum at Fort Meade, Maryland.



U.S. Government Photo

FIGURE 1-2

A U.S. Navy bombe machine designed to break the Enigma code on display at the National Security Agency's National Cryptologic Museum at Fort Meade, Maryland.

The Enigma system confounded Allied intelligence officials for years. The system was very complex and military officers were simply unable to break it. British mathematicians, led by Alan Turing, undertook an operation code-named Ultra that eventually broke the Enigma code. They used a very large, special-purpose computer, known as a *bombe* to break the code. An example of one of the bombes used by the U.S. Navy appears in Figure 1-2.

After breaking the Enigma code, Allied war planners gained great insight into German operations. They deciphered bombing targets while enemy planes were in the air. Navy officers read communications intended for German U-boats. The entire German communications system fell into Allied hands. Winston Churchill is famously quoted as telling King George VI that "It was thanks to Ultra that we won the war."

Cold War

The end of World War II marked the beginning of the cold war. This time of escalated tension between the United States and the Soviet Union lasted almost 50 years. The two superpowers postured with large stockpiles of nuclear weapons but rarely engaged in direct combat. Instead, one of the main characteristics of the cold war was the battles fought between intelligence officers. Many agencies on both sides developed significant intelligence capabilities. These included the use of spies, eavesdroppers, satellites, and spy planes.

The success of the Enigma program and the wide use of electronic communications after World War II led to the development of sophisticated electronic intelligence capabilities. The U.S. National Security Agency led the fight for the Americans, while the Committee on State Security (known by its Russian acronym, KGB) performed a similar function in the Soviet Union. Over the course of the cold war, both sides developed massive signals intelligence capabilities and became able to spy on each other's communications.

Intelligence played a role in almost every aspect of the cold war. During the Cuban Missile Crisis, President John F. Kennedy needed evidence that the Soviet Union was placing missiles in Cuba, very close to the Florida coast. He ordered Air Force spy planes to fly over the island, collecting valuable photos. These photos provided unmistakable evidence of missile activity.

Iraq War and Weapons of Mass Destruction

On the other hand, bad intelligence can have serious consequences. This became apparent during the war in Iraq that took place from 2003 to 2011. Before the war, U.S. and British officials claimed to have evidence that Iraq was developing weapons of mass destruction (WMD). Analysis after the war revealed that the programs had ended in the early 1990s, and that there was no credible evidence that Iraq was pursuing the WMD program that the Allies claimed.

In July 2002, several months before the March 2003 invasion of Iraq, British and American officials gathered in London to discuss war plans. In 2005, a copy of the minutes of that meeting was published in *The Sunday Times*. One section of those minutes quotes Richard Dearlove, the head of the British MI6 intelligence agency, as saying:

> Military action was now seen as inevitable. Bush wanted to remove Saddam, through military action, justified by the conjunction of terrorism and WMD. But the intelligence and facts were being fixed around the policy.

This was a damning accusation, as it asserted that military intelligence was being manipulated to tell the story that the government wanted people to hear. The intelligence community suffered reputational damage from this incident from which it took years to recover.

Domains of Warfare

Military planners have traditionally divided war-fighting capabilities into four domains. These domains are used to develop strategies and tactics as well as to organize forces. In fact, most modern militaries are organized according to these domains. The four domains of warfare are:

- **Land**—The oldest domain of warfare, consisting of any fighting force that remains on the ground. Land forces include infantry, cavalry, armored vehicles, antiaircraft batteries, and artillery. In the U.S. military, the United States Army primarily controls the land domain.
- **Sea**—The domain of warfare fought on oceans, rivers, and seas. The sea domain includes all of a nation's naval forces. In the U.S. military, the United States Navy controls the sea domain.
- **Air**—The domain of warfare fought in the sky. The air domain includes fighters, bombers, reconnaissance aircraft, cargo planes, and fuel tanker aircraft. After World War II, responsibility for the air domain in the U.S. military transferred from the Army to the Air Force.
- **Space**—With the advent of space flight, the military added space as a domain of warfare. The primary operations in this domain include satellite operations and the use of intercontinental ballistic missiles. In the U.S. military, the space domain is a mission of the Air Force.

NOTE

Although most people would consider helicopters aircraft, they are considered part of the land domain because they are primarily used in support of ground troops. For this reason, helicopter aviation is an Army mission.

NOTE

The United States Marine Corps is a military service that spans domains. Responsible for amphibious warfare, the Marine Corps fights in both the sea and land domains.

During the early stages of cyberwarfare, planners struggled with placing the cybermission into these domains and each service claimed responsibility for a portion of the mission. In 2010, a panel conducting the Quadrennial Defense Review for the U.S. Department of Defense (DoD) concluded that:

> Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.

With this statement, the military recognized the **cyber domain** as the fifth domain of warfare, as shown in Figure 1-3. Defense officials concluded that they must organize, equip, and train forces to operate in the cyber domain just as they do for the four traditional domains. Additionally, they recognized that they must be able to conduct their operations across the other domains in cases where use of the cyber domain is degraded by enemy action.

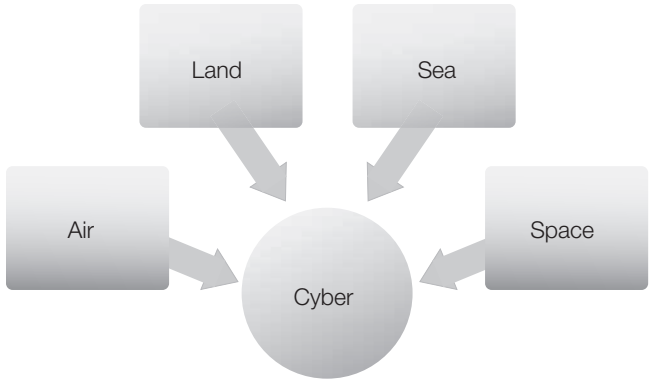


FIGURE 1-3
The relationship between the five domains of warfare.

Rather than creating a separate branch of the military to fight in the cyber domain, DoD reacted to this new domain by creating the **U.S. Cyber Command (USCYBERCOM)**. In the DoD *Strategy for Operating in Cyberspace*, the military outlines three needs that USCYBERCOM must fulfill for the military:

- "Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments;
- "Assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and
- "Ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most."

USCYBERCOM is responsible for conducting operations across all of the military services in these three areas of responsibility. The Director of the National Security Agency, a high-ranking military officer, commands USCYBERCOM.

Exploring the Cyber Domain

Cyber is a domain of warfare as significant as the other domains. As the newest domain of warfare, it is the least understood. Military planners specializing in land and sea operations have millennia of military history to draw upon when developing plans and strategies. Air and space have shorter histories as war-fighting domains but have still existed for over half a century. The cyber domain is much newer and military plans simply have not adapted fully to this new way of fighting.

The discussion of the cyber domain is organized around two major categories of information operations:

- **Offensive information operations**—Actions taken to deny, exploit, corrupt, or destroy an adversary's information or information functions
- **Defensive information operations**—Actions taken to protect your own information and information systems from an adversary's attempt to deny, exploit, corrupt, or destroy them

The combination of these two domains represents a full set of information operations capabilities that may be used by a military force to achieve its own objectives and prevent adversaries from achieving their own.

Offensive Information Operations

Offensive information operations are intentional military actions that are designed to adversely affect an enemy's information or information systems. There are four categories of offensive information operations objectives:

- *Deny* an adversary access to his or her own information or information systems.
- *Exploit* the sensitive information belonging to an adversary for your own military advantage.
- *Corrupt* information in an adversary's possession.
- *Destroy* the information or information systems an adversary relies on.

Offensive information operations may have one or more of the preceding objectives as goals. In all cases, the operations are designed to achieve specific military, political, or economic objectives that benefit the attacking force.

Defensive Information Operations

As with all domains of military operation, the cyber domain is two-sided. While militaries certainly seek to exploit the cyber domain to their advantage, they must also recognize that their adversaries are doing the same thing. In his 2010 *National Security Strategy*, President Barack Obama recognized this when he stated that:

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

If cyberspace is a national security issue, then the military must defend it as they would any other domain. This requires investing in military and civilian personnel with the skills required to operate in the cyber domain and equipping them with the tools necessary to meet their mission.

One distinguishing characteristic of cyberspace is the fact that military and civilian lines are blurred. In his risk statement above, President Obama cites power systems, the Internet, and e-commerce as critical assets. None of those assets is under military control. Therefore, a successful defense of the cyber domain requires partnerships between government and the private sector. Planning for defensive information warfare requires this coordination as well as international cooperation between allied countries.

Information Operations Techniques

Information operations are more than cyberwarfare. They include any activity undertaken to attack or protect information and information systems. This chapter considers seven categories of information operations techniques:

- Computer network attack
- Computer network defense
- Intelligence gathering
- Electronic warfare
- Psychological operations
- Military deception
- Operations security

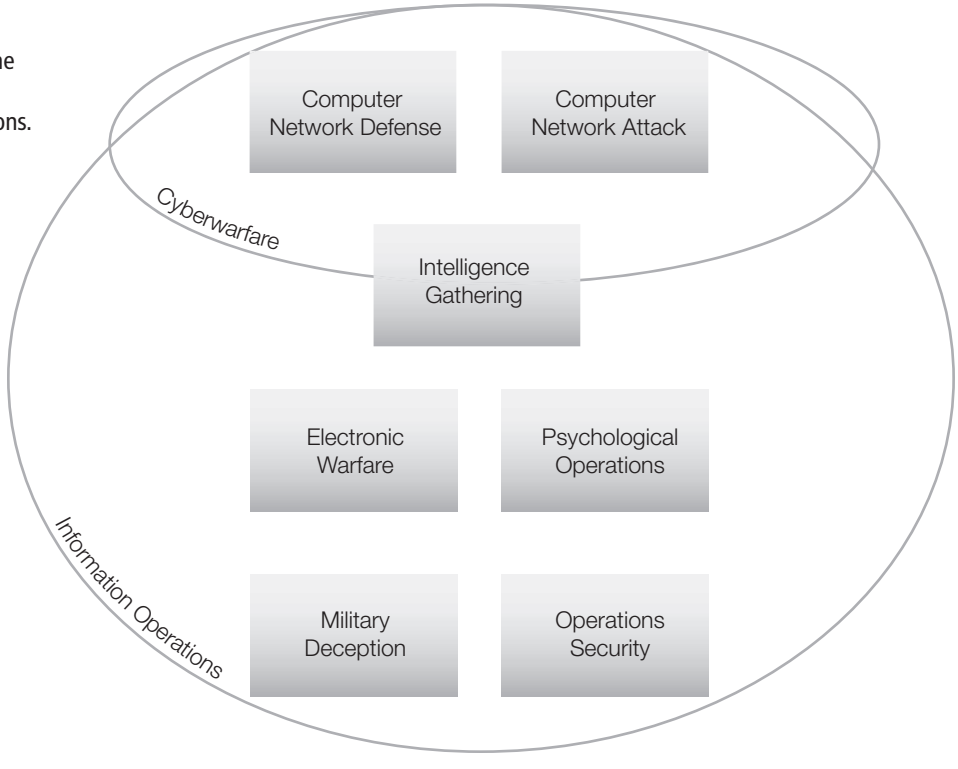


FIGURE 1-4
Cyberwarfare and the seven techniques of information operations.

These seven categories were outlined in the classified *Information Operations Roadmap* developed by the DoD in 2003. The *Roadmap* organized information operations into these categories and made specific recommendations about how the military might better organize, train, and equip to wage information operations in the future.

Figure 1-4 illustrates the relationship between these domains, cyberwarfare, and information operations. Notice that computer network defense and computer network attack fall squarely within the realm of cyberwarfare. They correspond to the cyberattack function discussed earlier in this chapter. Some intelligence-gathering activities fall within the cyber domain: specifically those that use cyberespionage techniques. However, while all intelligence gathering fits within the domain of information operations, not all intelligence operations are cyberwarfare.

Computer Network Attack

Computer network attack (CNA) is one of the core capabilities of offensive information operations and cyberwarfare. It consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy an adversary's information and/or information systems. As knowledge of a military's CNA capabilities provides helpful information to an adversary's defense efforts, governments are extremely reluctant to openly describe CNA activities, even in a theoretical sense.

The weapons used by military forces engaging in CNA activities are similar (and sometimes identical) to those hackers use in seeking to undermine information systems security. The significant financial and human resources of military forces provide them the ability to create CNA weapons that exploit vulnerabilities in computer systems and networks—vulnerabilities unknown to the outside world. These are known as **zero-day vulnerabilities** and are extremely difficult to defend against.

Edward Snowden and CNA Capabilities

The classified documents that Edward Snowden released to the media provided unprecedented insight into the CNA capabilities of the military forces of the United States and its allies. The capabilities Snowden revealed included:

- The ability to intercept communications between commercial data centers operated by Google and Yahoo! by tapping undersea communications cables
- Access to encrypted communications through weaknesses in commercial encryption algorithms
- Direct access to Microsoft, Yahoo!, Google, Facebook, AOL, Skype, YouTube, and Apple servers
- Ability to reveal sender identity information about some communications sent anonymously through The Onion Router (TOR) network

Although governments do not normally disclose CNA capabilities, the examples released by Snowden lead to the conclusion that CNA capabilities are extremely sophisticated. They reflect the investment of millions of dollars and countless hours of time and expertise in CNA techniques.

Computer Network Defense

Computer network defense (CND) activities are designed to protect, monitor, analyze, detect, and respond to unauthorized activity in friendly information systems and networks. This domain closely maps to the civilian field of information security, and there is a frequent exchange of talent and tools between the military and the private sector in this area.

Intelligence Gathering

Intelligence gathering is one of the core competencies of information operations. It includes efforts to gather information about an adversary's capabilities, plans, and actions. Military effectiveness is enhanced when leaders and planners have access to information about their adversary. Intelligence operations seek to obtain as much of this information as possible.

The domain of intelligence collection includes a wide variety of activities that collect intelligence using diverse sources and methods. When those methods include the exploitation of computer systems and networks, the activities fall under the category of cyberespionage and are part of both information operations and cyberwarfare.

Electronic Warfare

Electronic warfare includes all military actions designed to use electromagnetic or directed energy to either control the electromagnetic spectrum or attack the enemy. Examples of electronic warfare in practice include:

- Jamming enemy radio transmissions
- Disrupting the use of global navigation systems
- Placing false images on enemy radar screens or removing real images from those screens

Computer Network Exploitation

The cyberespionage capabilities of the U.S. military are commonly referred to using the term **computer network exploitation (CNE)**. CNE uses the capabilities of CNA to gain access to information systems and then infects them with malicious software designed to steal sensitive information on an ongoing basis.

The classified documents released by Edward Snowden revealed that the NSA has a specialized group, known as the Tailored Access Organization (TAO), that is dedicated to conducting this type of cyberwarfare. At the time of Snowden's disclosure, TAO had infiltrated more than 50,000 systems.

Foreign Policy magazine estimates that the TAO has approximately 600 employees who work at NSA headquarters in 24-hour shifts. Their activities include hacking into systems, cracking passwords, stealing data, and installing malicious software.

In Joint Publication 3-13.1, *Electronic Warfare*, the Joint Chiefs of Staff divide electronic warfare activities into three subdivisions:

- *Electronic attack* involves the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment. Electronic attacks intend to degrade, neutralize, or destroy enemy combat capabilities.
- *Electronic protect* includes actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of electronic warfare.
- *Electronic warfare support* includes actions taken to search for, intercept, identify, and locate sources of electromagnetic radiation. This is done for threat recognition, targeting, planning, and engaging in electronic attack operations.

Electronic warfare is waged using a wide variety of weapons systems, including fixed ground stations, specialized aircraft, and ships at sea. The U.S. military has been conducting electronic warfare operations for decades and has entire units dedicated to the electronic warfare mission.

Psychological Operations

Psychological operations (PSYOPs) are defined by the U.S. military as military operations planned to convey selected information and indicators to foreign governments, organizations, groups, and individuals in order to influence their emotions, motives, objective reasoning, and behavior. In the Army Field Manual *Psychological Operations*, the military outlines five roles for PSYOPs:

NOTE

Although most of the world continues to call this domain PSYOPs, the U.S. military recently shifted to using the more innocuous-sounding term Military Information Support Operations (MISO) in its place.

- Influence foreign populations by sharing information subjectively. The information shared is designed to influence the population's attitudes and behavior and obtain compliance or other desired changes in behavior.
- Advise military commanders on ways to conduct military actions in a way that attacks the enemy's will to resist and minimizes the adverse impacts on psychological targets.
- Provide public information to foreign populations to support humanitarian activities, restore or reinforce legitimacy, ease suffering, and maintain or restore civil order.
- Serve as the commander's voice to foreign populations to convey intent and establish credibility.
- Counteract enemy propaganda to portray friendly intent and actions in a positive light for foreign audiences.

Propaganda is one of the major tools of psychological operations, and it may take place in oral or written form. Some of the most famous propaganda attacks against the United States military include the "Tokyo Rose" radio broadcasts from Japan to U.S. troops during World War II and the "Hanoi Hannah" broadcasts used by the Viet Cong during the Vietnam War.

FIGURE 1-5

American propaganda leaflet distributed to the population of Germany during World War II.

U.S. Government Leaflet

Figure 1-5 shows an example of written propaganda used by the U.S. government during World War II. This leaflet, intended for the German population, includes the headline question, "Do you want total war?" It goes on to tell the German people that they must choose between destruction and total war under the Nazis or normal and peaceful development under the Allies.

Military Deception

Military deception actions are designed to mislead adversary forces about the operational capabilities, plans, and actions of friendly forces. The goal of military deception is to guide the adversary toward taking actions desired by the entity engaging in deception. Military deception may occur at the strategic level, attempting to mislead foreign leaders into making tremendous strategic mistakes. It also may occur at the tactical level, with field commanders trying to mislead each other about their intentions.

Operations Security

Operations security (OPSEC) activities are designed to deny an adversary access to information about friendly forces that would reveal capabilities, plans, or actions. It is designed to prevent the enemy from successfully engaging in intelligence gathering. The OPSEC process has five components, shown in Figure 1-6. They are outlined in Joint Publication 3-13.3: *Operations Security*.

Operation Bodyguard

Both sides made significant use of deception during World War II. One significant military deception campaign was Operation Bodyguard, which took place in 1944. It consisted of a series of coordinated deception efforts led by the Allied Powers designed to mislead the Germans about the time and location of the impending Allied invasion at Normandy.

Several different operations, code-named Fortitude, Graffham, Ironside, Zeppelin, and Copperhead, engaged in various deception tactics to paint a full, but incorrect, picture for the Germans. They used false radio signals, decoy actors, double agents, and false export restriction requests to mislead the Germans and cause them to structure forces in a manner that facilitated the Normandy landing.

The Operation Ultra intercepts of German Enigma communications mentioned earlier in this chapter also played a role in Bodyguard. The Allies had access to German communications and were able to tell which deception efforts were succeeding in misleading German commanders.

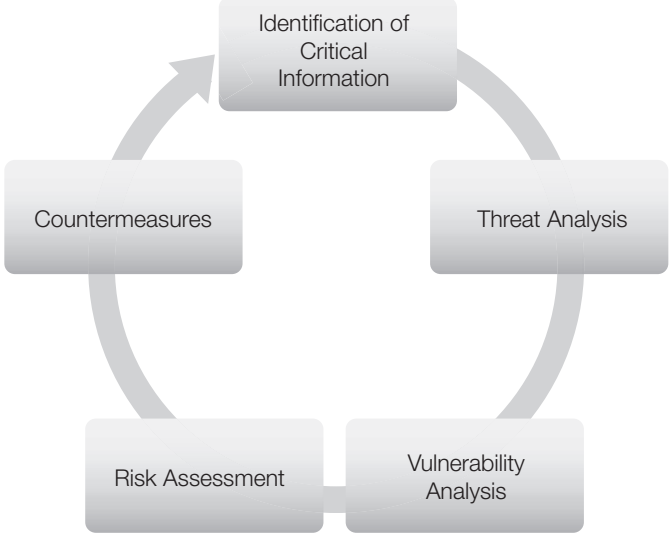


FIGURE 1-6
Steps in the operations security process.

Identification of Critical Information

During the first phase of the OPSEC process, analysts seek to identify the essential information elements that would be valuable to the enemy and cause harm if disclosed. It is crucial that analysts identify this information because it allows the remainder of the process to protect only critical information, rather than trying to safeguard voluminous amounts of nonsensitive information.

The critical information identification process includes a wide variety of military staff representing different military disciplines. The work product of this phase is a document known as the critical information list (CIL).

Threat Analysis

After developing the CIL, operations planners conduct research based upon collected intelligence, knowledge of adversary intelligence capabilities, and publicly available information. The purpose of this analysis is to answer six fundamental questions:

- Who is the adversary?
- What are the adversary's goals?
- What is the adversary's likely course of action?
- What critical information does the adversary already know?
- What are the adversary's intelligence-gathering capabilities?
- Who will share information with the adversary?

The answers to these questions allow OPSEC planners to paint an informed picture of the adversary that may be compared with vulnerabilities in friendly forces during the risk assessment.

Vulnerability Analysis

During the vulnerability analysis, OPSEC planners examine every aspect of a planned operation to identify the ways that an adversary could gather pieces of critical information from the operation. Vulnerabilities exist when friendly forces provide adversaries with the opportunity to collect critical information, analyze it, and take action on it. The vulnerability analysis phase is focused on **indicators**, friendly actions and information that reveal critical information to the enemy.

The vulnerability analysis phase is designed to answer four questions:

- What indicators of critical information will be created by friendly activities?
- Which of those indicators can the adversary actually collect?
- What indicators will the adversary be able to use to the disadvantage of friendly forces?
- Will the use of OPSEC countermeasures actually tip the adversary off to more critical information?

Parking Lot Intelligence

OPSEC indicators come in the strangest places. One tried-and-true vulnerability that an adversary might use is to simply count the number of cars in government parking lots. The presence of an unusual number of people after hours may indicate imminent military activity.

Risk Assessment

During the risk assessment phase, OPSEC planners perform a thorough assessment of the information collected in the first three phases and the countermeasures that may be used to limit the ability of adversaries to collect those indicators. Planners then perform a cost-benefit analysis to identify which, if any, countermeasures should be implemented.

OPSEC planners perform three steps while conducting a risk assessment:

1. Analyze the vulnerabilities identified during the vulnerability assessment and identify possible OPSEC countermeasures for each.
2. Estimate the cost of implementing each OPSEC countermeasure (in terms of time, cost, and impact on operations) and compare it with any harmful effects that would result if an adversary exploits the vulnerability.
3. Select OPSEC countermeasures for execution.

The use of risk assessment allows commanders to make informed decisions about OPSEC countermeasures with knowledge of the associated costs.

Countermeasure Implementation

After selecting appropriate countermeasures during the risk assessment, commanders then execute the OPSEC plan. The overall strategy should meet four criteria:

- Minimize predictability from previous operations.
- Identify indicators that may tip the adversary off to the OPSEC activities.
- Conceal indicators of key capabilities and military objectives.
- Counter vulnerabilities in mission processes and technologies.

Once the OPSEC countermeasures are in place, OPSEC staff should monitor enemy reactions to identify whether the countermeasures are effective and feed this information back into the planning process.

CHAPTER SUMMARY

In this chapter, you learned the fundamentals of cyberwarfare and how information is a military asset. Cyberwarfare includes a wide range of activities that use information systems as weapons against an opposing force. It includes cyberattacks—designed to cause physical or electronic damage to information systems—and cyberespionage—intrusions into computer systems and networks designed to steal sensitive information. Cyberwarfare activities are a subset of the larger field of information warfare and information operations—activities that encompass all of the ways information affects military operations. Cyberwarfare is the latest step in the natural evolution of warfare. As societies have become more dependent upon information technology, so have their militaries, and this technological independence creates an opportunity to militarize cyber as the fifth domain of warfare. In this way, cyber complements the existing warfare domains of land, sea, air, and space.

There are seven major categories of information operations techniques. Computer network attack and computer network defense attempt to exploit and defend technology systems. Intelligence gathering has the goal of obtaining information about an adversary. Electronic warfare attempts to use the electromagnetic spectrum as a weapon. Psychological operations and military deception seek to sway and mislead enemy forces and leaders. Operations security seeks to deny adversaries access to critical elements of friendly information.

KEY CONCEPTS AND TERMS

Computer network attack (CNA)
Computer network defense (CND)
Computer network exploitation (CNE)
Cyberattacks
Cyber domain
Cyberespionage
Cyberwarfare
Electronic warfare
Indicators
Information operations
Information warfare
Intelligence gathering
Military deception
Nonstate actors
Operations security (OPSEC)
Psychological operations (PSYOPs)
U.S. Cyber Command (USCYBERCOM)
Zero-day vulnerabilities

CHAPTER 1 ASSESSMENT

1. Information warfare first appeared in the late part of the twentieth century.

A. True
B. False

2. Which one of the following is the newest domain of warfare?

A. Air
B. Land
C. Sea
D. Cyber
E. Space

3. What are the two major categories of cyberwarfare? (Select two.)

A. Viruses
B. Cyberattack
C. Cyberespionage
D. Firewalls

4. The U.S. agency most closely associated with waging cyberwarfare is the _____.

A. FBI
B. NSA
C. CIA
D. DNI

5. All information warfare activities are examples of cyberwarfare.

A. True
B. False

6. What was the name of the British and American effort to break German cryptography during World War II?

A. Ultra
B. Enigma
C. Purple
D. Green

7. The evidence used to prove that the Soviet Union was building secret missile bases in Cuba was gathered by _____.

A. Satellites
B. Human spies
C. Wiretapping
D. Spy planes

8. What joint command of the U.S. military has primary responsibility for operations that take place in the cyber domain?

A. USCENTCOM
B. USEURCOM
C. USSTRATCOM
D. USCYBERCOM

9. Which of the following techniques include capabilities related to the conduct of cyberwarfare? (Select three.)

A. Intelligence gathering
B. Electronic warfare
C. Computer network attack
D. Psychological operations
E. Computer network defense

10. It is extremely difficult to defend against an attacker who is exploiting a zero-day vulnerability.

A. True
B. False

11. All intelligence-gathering operations are examples of information operations.

A. True
B. False

12. What discipline includes activities designed to deny an adversary access to information about friendly capabilities, plans, and objectives?

A. OPSEC
B. Electronic warfare
C. PSYOPS
D. CNA

13. During which phase of the OPSEC process does the commander select appropriate OPSEC countermeasures?

A. Vulnerability assessment
B. Risk assessment
C. Threat assessment
D. Countermeasure implementation

14. What discipline includes actions taken to search for, intercept, identify, and locate sources of electromagnetic radiation?

A. Electronic attack
B. Electronic warfare support
C. Electronic protect
D. Electronic intelligence

15. What name is used to describe the process of gaining access to information systems and then infecting them with malicious software designed to steal sensitive information on an ongoing basis?

A. CNA
B. CND
C. CNE
D. CNY