TT TEXTBOOK TESTBANKS

Test Bank for Cyberwarfare: Information Operations in a Connected World 2nd Chapple

TEST BANK SAMPLE PREVIEW

PUBLISHER

JBLearning

COPYRIGHT

2022

RESOURCE TYPE

Test Bank

ISBN

9781284225440

Test Bank for Cyberwarfare-Information Operations in a Connected World 2nd Edition by Chapple, Seidl

ISBN: 9781284225440

Cyberwarfare: Information Operations in a Connected World, Second Edition
Mike Chapple and David Seidl

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284228311, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. What is a form of cyberwarfare that is a nonkinetic, offensive operation intended to cause some form of physical or electronic damage?
A) Operations security
B) Intelligence gathering
C) Cyberattack
D) Computer network defense
Ans: C
Complexity: Moderate
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy: Understand

2. What are the two major activities of cyberwar?
A) Information operations and cyberattacks
B) Cyberespionage and military deception
C) Cyberattacks and cyberespionage
D) Psychological operations and cyberespionage
Ans: C
Complexity: Moderate
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: A threat assessment of cyberwarfare by the United States Director of National Intelligence (DNI) 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 and cyberespionage.
Taxonomy: Recall

3. Selena is a cybersecurity expert for the U.S. Department of Defense. She is investigating a case in which an unknown party installed ransomware in the computer systems of a critical national utility. She discovers that the group claiming responsibility does not represent a national government. The group considers itself to be a type of cyberactivist. What is such a person or group called?
A) Cyber command
B) Nonstate actor
C) Military cyber operations
D) Psychological operations
Ans: B
Complexity: Moderate
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Nonstate actors are individuals or groups that seek to participate in cyberwarfare but do so independently, without the endorsement of a national government.
Taxonomy: Apply

4. Which of the following is *not* an example of an event marking the turning point in the evolving history of warfare?
A) The use of written documents by Julius Caesar to communicate with his troops on the battlefield
B) Colonists using guerrilla warfare against the British army in 1775
C) A computer worm being used to sabotage Iran's nuclear enrichment facility in 2010
D) The use of nuclear weapons by the U.S. military against Japan in 1945
Ans: A
Complexity: Moderate
Ahead: The Evolving Nature of War
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The use of written documents for communications between leaders and troops was not a turning point in warfare.
Taxonomy: Analyze

5. Which military service is responsible for amphibious warfare, fighting in both the land and sea domains?
A) U.S. Air Force
B) U.S. Army
C) U.S. Marine Corps
D) U.S. Navy
Ans: C
Complexity: Easy
Ahead: Domains of Warfare
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy: Recall

6. Which piece of military equipment is considered part of the land domain?
A) Battleship
B) Helicopter
C) Stealth bomber

D) Submarine
Ans: B
Complexity: Easy
Ahead: Domains of Warfare
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: 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.
Taxonomy: Understand

7. Arturo is a cybersecurity advisor for the U.S. Department of Defense. He is planning to use an enemy's information to the advantage of the U.S. military. What type of strategy is this called?
A) Denial
B) Exploitation
C) Corruption
D) Destruction
Ans: B
Complexity: Moderate
Ahead: Exploring the Cyber Domain
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Offensive information operations include actions taken to exploit an enemy's sensitive information to the advantage of the U.S. military.
Taxonomy: Apply

8. Tonya is evaluating the activities of a cyber information system. The system has the capabilities to intercept communications between commercial data centers, access encrypted communications, and reveal sender identities of people using The Onion Router (TOR) network system. According to the U.S. Department of Defense's *Information Operations Roadmap*, what type of information operation technique is Tonya most likely evaluating?
A) Computer network attack (CNA)
B) Computer network defense (CND)
C) Psychological operations (PO)
D) Operations security (OS)
Ans: A
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: These activities involve CNA and are examples of events previously disclosed to news agencies by Edward Snowden.
Taxonomy: Analyze

9. According to the U.S. Department of Defense's *Information Operations Roadmap*, what type of information operation technique operates within the realms of cyberwarfare and information operations?
A) Intelligence gathering
B) Armed conflict
C) Electronic warfare
D) Operations security
Ans: A

Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: 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.
Taxonomy: Understand

10. Which of the U.S. Department of Defense's seven techniques of information operations may involve disrupting the use of global navigation systems and jamming enemy radio transmissions?
A) Computer network defense
B) Intelligence gathering
C) Electronic warfare
D) Military deception
Ans: C
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: 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, and placing false images on enemy radar screens or removing real images from those screens.
Taxonomy: Understand

11. Which of the U.S. Department of Defense's seven techniques of information operations involves counteracting enemy propaganda to portray friendly intent and actions in a positive light for foreign audiences?
A) Operations security
B) Intelligence gathering
C) Military deception
D) Psychological operations
Ans: D
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: One of the five roles of psychological operations (PSYOPs) is to counteract enemy propaganda to portray friendly intent and actions in a positive light for foreign audiences.
Taxonomy: Understand

12. In 1942, British General Montgomery manipulated strategic information about the timing of an attack against German General Rommel. What is this type of strategy called, according to the U.S. Department of Defense's *Information Operations Roadmap*?
A) Operations security
B) Military deception
C) Psychological operations
D) Intelligence gathering
Ans: B

Complexity: Difficult
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The goal of military deception is to guide the adversary toward taking actions desired by the entity engaging in deception, which can involve deceiving foreign leaders and leading them toward making strategic mistakes.
Taxonomy: Understand

13. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. What is *not* one of the five primary steps of OPSEC?
A) Identification of critical information
B) Threat analysis
C) Intelligence gathering
D) Countermeasures
Ans: C
Complexity: Easy
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The five primary steps of OPSEC are identification of critical information, threat analysis, vulnerability analysis, risk assessment, and countermeasures. Intelligence gathering is not one of the five primary steps.
Taxonomy: Recall

14. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. Why do 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?
A) To protect only critical information, rather than trying to safeguard voluminous amounts of nonsensitive information
B) To protect all information, whether critical or nonsensitive
C) To determine whether the information is offensive or defensive
D) To perform a vulnerability analysis determining when our forces may provide adversaries with critical information
Ans: D
Complexity: Difficult
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: All aspects of a planned operation must be evaluated to understand what an adversary could learn from each aspect. When any aspect reveals information that could be of use to an adversary, it should be modified to eliminate or mitigate such disclosures. This is a key part of what a vulnerability analysis will reveal.
Taxonomy: Analyze

15. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. Which phase of the OPSEC process involves a series of questions that help identify adversaries and their capabilities?
A) Identification of critical information
B) Threat analysis

C) Vulnerability analysis
D) Risk assessment
Ans: B
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: During the threat analysis phase of the OPSEC process, operations planners conduct research based on collected intelligence, knowledge of adversary intelligence capabilities, and publicly available information. The purpose of this analysis is to answer questions that help paint an informed picture of the adversary, and the potential threats they might pose.
Taxonomy: Understand

16. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. During which phase of the OPSEC process is a cost-benefit analysis conducted?
A) Identification of critical information
B) Threat analysis
C) Vulnerability analysis
D) Risk assessment
Ans: D
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: 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.
Taxonomy: Understand

17. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. Which phase of the OPSEC process focuses on indicators, friendly actions and information that reveal critical information to the enemy? During this phase, questions are asked such as "what indicators of critical information will be created by friendly activities" and "which of those indicators can the adversary actually collect?"
A) Identification of critical information
B) Threat analysis
C) Vulnerability analysis
D) Risk assessment
Ans: C
Complexity: Difficult
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: During the vulnerability analysis phase, OPSEC planners examine every aspect of a planned operation to identify the ways that an adversary could gather pieces of critical information, including asking critical questions to resolve the analysis. This phases focuses on indicators.
Taxonomy: Understand

18. Operations security (OPSEC) is one of the U.S. Department of Defense's techniques of information operations. In the OPSEC process, in what context does a vulnerability exist?
A) When information is identified as critical
B) When adversaries attempt to collect information
C) When friendly forces collect critical information, analyze it, and take action on it
D) When friendly forces provide adversaries with the opportunity to collect critical information, analyze it, and take action on it
Ans: D
Complexity: Difficult
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: If friendly forces disclose critical information, they give adversaries the opportunity to analyze and interpret such information, and possibly to act on those results. Because this could expose friendly forces to negative outcomes, these disclosures present unwanted vulnerabilities.
Taxonomy: Understand

19. What are the four categories of offensive information operations objectives of the U.S. military's cyber domain?
A) Identify, exploit, corrupt, and dismiss
B) Deny, exploit, corrupt, and destroy
C) Deny, exploit, corrupt, and dismiss
D) Identify, deny, attack, and destroy
Ans: B
Complexity: Moderate
Ahead: Exploring the Cyber Domain
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Deny means to withhold or negate information or actions. Exploit means to take direct advantage of an adversary’s weakness or exposure. Corrupt means to degrade, destroy, or confuse adversary capabilities or information. Destroy means to severely damage or eliminate adversary capabilities or information. Other answers include non-offensive terms, specifically “identify” and “dismiss.”
Taxonomy: Analyze

20. During World War II, the Allied Powers used techniques such as sending false radio signals and using decoy actors, double agents, and false export restriction requests as part of Operation Bodyguard. What was this an example of?
A) Electronic warfare
B) Intelligence gathering
C) Military deception
D) Warfare domains
Ans: C
Complexity: Easy
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: 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.
Taxonomy: Understand

True/False

1. True or False? Cyberwarfare is exclusively focused on stealing sensitive information that may be used for military, political, or economic gain.
Ans: False
Complexity: Easy
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Cyberwarfare includes a wide range of activities that use information systems as weapons against an opposing force.
Taxonomy:

2. True or False? A computer virus designed to disrupt the control systems of an unmanned aerial vehicle, such as a drone, is an example of a cyberattack.
Ans: True
Complexity: Easy
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

3. True or False? The Church of Scientology is an example of a nonstate actor.
Ans: False
Complexity: Moderate
Ahead: What Is Cyberwarfare?
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The group Anonymous, which is an example of a nonstate actor, has targeted the Church of Scientology. The Church of Scientology itself has not been identified as a cyberwarfare actor.
Taxonomy:

4. True or False? During World War II, the United States and British governments developed the Enigma machine to encrypt messages.
Ans: False
Complexity: Easy
Ahead: The Role of Information in Armed Conflict
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The German and Japanese governments developed the Enigma machine to encrypt messages.
Taxonomy:

5. True or False? The end of World War II marked the beginning of the Cold War, a 50-year period in which tensions escalated between the United States and North Korea.
Ans: False
Complexity: Moderate
Ahead: The Role of Information in Armed Conflict
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: During the Cold War, tensions escalated between the United States and the Soviet Union.
Taxonomy:

6. True or False? The four domains of traditional warfare are land, sea, air, and cyber.
Ans: False
Complexity: Moderate
Ahead: Domains of Warfare
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The four domains of traditional warfare are land, sea, air, and space. Cyber was added in 2010.
Taxonomy:

7. True or False? In the U.S. military, the space domain is a mission of the Air Force.
Ans: True
Complexity: Easy
Ahead: Domains of Warfare
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

8. True or False? Defensive information operations are intentional military actions that are designed to adversely affect an enemy's information or information systems.
Ans: False
Complexity: Difficult
Ahead: Exploring the Cyber Domain
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Offensive information operations are intentional military actions that are designed to adversely affect an enemy's information or information systems. Defensive information operations protect against such actions.
Taxonomy:

9. True or False? According to the U.S. Department of Defense's *Information Operations Roadmap*, while all intelligence gathering fits within the domain of information operations, not all intelligence operations are cyberwarfare.
Ans: True
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1

Title: Information as a Military Asset
Feedback:
Taxonomy:

10. True or False? A vulnerability in a computer system or network that is unknown to the outside world is known as a zero-day vulnerability.
Ans: True
Complexity: Easy
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

11. True or False? According to the U.S. Department of Defense's *Information Operations Roadmap*, computer network attack (CNA) activities are designed to protect, monitor, analyze, detect, and respond to unauthorized activity in friendly information systems and networks.
Ans: False
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: According to the *Roadmap*, computer network defense (CND) activities are designed to protect, monitor, analyze, detect, and respond to unauthorized activity in friendly information systems and networks.
Taxonomy:

12. True or False? The cyberespionage capabilities of the U.S. military are commonly referred to using the term "computer network exploitation" (CNE).
Ans: True
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

13. True or False? According to the U.S. Department of Defense, when intelligence gathering efforts include the exploitation of computer systems and networks, the activities fall under the category of cyberespionage.
Ans: True
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

14. True or False? 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.
Ans: True
Complexity: Easy
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

15. True or False? Military deception may occur at the strategic level, attempting to mislead foreign leaders into making tremendous strategic mistakes.
Ans: True
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

16. True or False? Propaganda was historically used in warfare but is no longer a significant tool in military operations.
Ans: False
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Propaganda remains a major tool of military psychological operations.
Taxonomy:

17. True or False? Electronic warfare may involve placing false images on enemy radar screens.
Ans: True
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback:
Taxonomy:

18. True or False? The "Hanoi Hannah" broadcast used by the Viet Cong during the Vietnam War is an example of a propaganda attack.
Ans: True
Complexity: Easy
Ahead: Information Operations Techniques
Subject: Chapter 1

Title: Information as a Military Asset
Feedback:
Taxonomy:

19. True or False? During the vulnerability analysis phase of the U.S. military's operations security (OPSEC) process, planners perform a cost-benefit analysis to identify which, if any, countermeasures should be implemented.
Ans: False
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: The cost-benefit analysis occurs during the risk assessment phase.
Taxonomy:

20. True or False? During the U.S. military's operations security (OPSEC) process, once a countermeasure is put in place, it is not changed.
Ans: False
Complexity: Moderate
Ahead: Information Operations Techniques
Subject: Chapter 1
Title: Information as a Military Asset
Feedback: Once an OPSEC countermeasure is in place, OPSEC staff monitor enemy reactions to identify whether the countermeasure is effective and feed this information back into the planning process. Changes are constantly considered and often introduced in response to their analyses.
Taxonomy: