Lesson 2 Progress

✓   Quiz submitted   ✕

- Due No due date
- Points 100
- Questions 10
- Time Limit 15 Minutes
- Allowed Attempts Unlimited

Instructions

This quiz checks your understanding of lesson concepts.

- This is a timed assessment.
- You are allowed multiple attempts.
- Minimum passing score is 80%.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	**Attempt 1**	11 minutes	70 out of 100

⊙ Correct answers are hidden.

Score for this attempt: 70 out of 100
Submitted Nov 2 at 9:03am
This attempt took 11 minutes.

Question 1

10 / 10 pts

✓ Quiz submitted

In what aspect does cyberspace fundamentally differ from other domains?

○ Cyberspace operates in real-time, allowing for instantaneous communication and interaction.

○ It is inherently decentralized, unlike the hierarchical structures of land, sea, and air.

◉ Cyberspace is man-made, distinct from the natural characteristics of land, sea, and air.

○ Unlike other domains, cyberspace is governed by a complex network of international agreements and treaties.

This answer is correct.

Question 2

10 / 10 pts

In the context of potential future conflicts, how might adversaries seek to undermine America's military superiority?

○ By employing asymmetrical guerrilla tactics to disrupt cyber operations and military strategies.

○ By intensifying information operation efforts to erode public support for military actions.

◉ Through offensive cyberspace campaigns aimed at disrupting America's war-fighting capabilities.

○ Through the deployment of advanced digital weaponry systems.

This answer is correct.

IncorrectQuestion 3

0 / 10 pts

In the article, "Cyberspace – The Fifth Operational Domain," by Larry Welch, he discusses how the level and scope of the need for control of cyberspace is dependent on the activity conducted in, through, and from cyberspace. In general, there are six classes of activities. Which activity is one of the six?

○ Mutual defense

○ Constructing cyberspace

◉ Data exploitation

This answer is incorrect. In Larry Welch's article, "Cyberspace — The Fifth Operational Domain," he says environment exploitation is one of the six classes of activities. (Sour

☑ **Quiz submitted**

○ Active offense

⠿

Question 4

10 / 10 pts

What significant event prompted the first-ever US retaliation against a foreign cyber attack on a US company?

○ The disruption of critical infrastructure systems, leading to widespread power outages.

◉ The intrusion into a movie studio's network.

○ The hacking of a major financial institution's database resulting in significant data breaches.

○ The theft of intellectual property from a leading technology company.

This answer is correct.

⠿

IncorrectQuestion 5

0 / 10 pts

According to Yeremyan, why is it often difficult or even impossible to ascertain the source of a cyber attack?

◉ Cyber attacks often utilize anonymizing technologies, making source attribution elusive or impractical.

○ Due to the decentralized and interconnected nature of cyberspace.

○ Due to the vast number of potential attack vectors, narrowing down the source becomes challenging.

○ The lack of comprehensive cybersecurity protocols hampers forensic investigations.

This answer is incorrect. Please review Lesson 2, Objective 2.

⠿

IncorrectQuestion 6

0 / 10 pts

According to Siboni and Sevila, which civilian sector is considered the most vulnerable to cybercrime due to its pivotal role in societal functioning?

○ Critical Infrastructure

○ Finance and Banking

○ Parks and Recreation

◉ Healthcare

✓ Quiz submitted

This answer is incorrect. Please review Lesson 2, Objective 2.

⋮⋮

Question 7

10 / 10 pts

The DoD Cyber Strategy establishes four complementary objectives for cyberspace. From the answers below, which one is **NOT** one of the four objectives?

○ Protect the cyber domain with allies and partners.

◉ Penetrate hostile networks.

○ Defend the nation.

○ Build enduring advantages in cyberspace.

This answer is correct.

⋮⋮

Question 8

10 / 10 pts

What action did the IoT Cybersecurity Improvement Act of 2020 primarily direct?

○ Mandating strict cybersecurity standards for IoT manufacturers.

○ Establishing a federal agency dedicated solely to IoT security oversight.

○ Allocating funding to train cybersecurity professionals in IoT-specific threats.

◉ Improving IoT cybersecurity through Federal research and development, procurement, and risk management efforts.

This answer is correct.

⋮⋮

Question 9

10 / 10 pts

According to the DoD *Cyber Strategy, the Department of Defense's strategic approach is based on four* complementary objectives. The fourth objective in this approach i[ ] which is the first stated goal to achieve this objective?

Quiz submitted

○ Plan for network defense and resilience.

○ Mitigate known vulnerabilities in personnel and systems.

○ Develop the unified systems platform.

◉ Invest in the cyber workforce.

This answer is correct.

⁞

Question 10

10 / 10 pts

The National Cyber Strategy of the United States, issued by the White House, contains five pillars that will guide United States cyber operations. From the answers below, which one is a correct pillar?

○ Counter Russia and Iran

◉ Invest in a Resilient Future

○ Spread democracy

○ Defeat cyber criminals

This answer is correct.

Quiz Score: 70 out of 100