Question 1 (1 point) ✓ *Saved*

Which phase of the operations security (OPSEC) process involves a series of questions that helps identify adversaries and their capabilities?

- identification of critical information
- threat analysis
- vulnerability analysis
- risk assessment

Question 2 (1 point) ✓ *Saved*

During which phase of the intelligence cycle is a collection plan created?

- Planning and Direction
- Collection
- Processing and Exploitation
- Analysis and Production
- Dissemination

Question 3 (1 point) ✓ *Saved*

The U.S. Air Force is responsible for which domains of warfare?

- land and sea
- sea and air
- air and space
- space and sea

Question 4 (1 point) ✓ *Saved*

In Operation Eligible Receiver, the attacker used social engineering techniques to trick a victim at the targeted company into visiting a malicious Web site.

- ◯ True
- ◯ False

Question 5 (1 point) ✓ *Saved*

Because cyberattackers never reveal themselves, social media is not an effective tool for identifying cyberattackers.

- ◯ True
- ◯ False

Question 6 (1 point) ✓ *Saved*

The term hacker once described an individual who was extremely proficient at manipulating computers.

- ◯ True
- ◯ False

Question 7 (1 point) ✓ *Saved*

Which of the U.S. Department of Defense's (DoD's) seven techniques of information operations is designed to prevent the enemy from successfully engaging in intelligence gathering?

- ◯ operations security
- ◯ intelligence gathering
- ◯ electronic warfare
- ◯ computer network defense

Question 8 (1 point) ✓ *Saved*

The laws of warfare are based on disagreement.

- ◯ True
- ◯ False

Question 9 (1 point) ✓ *Saved*

Which of the following attacks take advantage of a concept known as the window of vulnerability?

- ◯ Zero-day attack
- ◯ Malware
- ◯ Phishing
- ◯ Strategic Web compromise

Question 10 (1 point) ✓ *Saved*

When intelligence gathering 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.

- ◯ True
- ◯ False

Question 11 (1 point) ✓ *Saved*

Although the civilian communication infrastructure was traditionally a part of intelligence-gathering missions, it is now likely to be directly targeted by military cyberwarfare teams, activists, and other hackers as well

- ◯ True
- ◯ False

Question 12 (1 point) ✓ *Saved*

_____ warfare is fought using all available resources. Traditional rules of war are set aside, and civilian and military targets are considered acceptable.

- ◯ Conventional
- ◯ Unconventional
- ◯ Asymmetric
- ◯ Total

Question 13 (1 point) ✓ *Saved*

The four common advanced persistent threat (APT) motivations are military/political, government espionage, treachery, and pacifism.

- ◯ True
- ◯ False

Question 14 (1 point) ✓ *Saved*

Which of the following is NOT true of the Moonlight Maze attacks?

- ◯ They began in March 1998 and were not detected by the government until the spring or summer of 1999.
- ◯ Some of the attacks were traced back to a computer system located in Russia
- ◯ Thousands of files may have been stolen during the attacks.
- ◯ They impacted only systems running Microsoft Internet Information Server (IIS) Web server software.

Question 15 (1 point) ✓ *Saved*

Which intelligence discipline is least likely to help intelligence professionals gather information about a well-organized and large hacktivist group that is planning to deface several government Web sites?

- ◯ geospatial intelligence (GEOINT)
- ◯ human intelligence (HUMINT)
- ◯ open source intelligence (OSINT)
- ◯ financial intelligence (FININT)

Question 16 (1 point) ✓ *Saved*

_____ is a loosely organized group of activist hackers who orchestrate distributed denial of service (DDoS) attacks against targets they select based upon ideological concerns, such as organizations associated with antipiracy efforts on the Internet.

- ◯ The Syrian Electronic Army (SEA)
- ◯ Anonymous
- ◯ PRISM
- ◯ Echelon

Question 17 (1 point) ✓ *Saved*

Regarding the operations security (OPSEC) process, in what context does a vulnerability exist?

- ◯ When information is identified as critical
- ◯ When adversaries attempt to collect information
- ◯ When friendly forces collect critical information, analyze it, and take action on it
- ◯ When friendly forces provide adversaries with the opportunity to collect critical information, analyze it, and take action on it

Question 18 (1 point) ✓ *Saved*

Major security investments may be easily undermined if organizations overlook which of the following single weak link in them all?

- ◯ software updates
- ◯ security training
- ◯ firewall implementation
- ◯ human factors

Question 19 (1 point) ✓ *Saved*

Cyberwarfare combatants are limited to military personnel and intelligence operatives.

- ◯ True
- ◯ False

Question 20 (1 point) ✓ *Saved*

The principle of social liking states that once someone has made a commitment to a particular course of action, that person becomes confident that his or her action was correct and consistent.

- ◯ True
- ◯ False

Question 21 (1 point) ✓ *Saved*

During the Planning and Direction phase of the intelligence cycle, what are intelligence requirements?

- ◯ Plans for disposing of faulty or old intelligence
- ◯ General or specific subjects for which there is a need for information collection or intelligence production
- ◯ Plans for analyzing massive amounts of data collected by intelligence assets
- ◯ Guidelines for intelligence analysts to use when examining information from a variety of intelligence sources

Question 22 (1 point) ✓ *Saved*

Advanced persistent threats (APTs) are highly organized and have significant resources at their disposal.

- ◯ True
- ◯ False

Question 23 (1 point) ✓ *Saved*

According to the U.S. Department of Defense's (DoD'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.

- ◯ True
- ◯ False

Question 24 (1 point) ✓ *Saved*

Existing international law specifically mentions military action, making the involvement of a military group or organization more likely to result in the action being considered a use of force.

- ◯ True
- ◯ False

Question 25 (1 point) ✓ *Saved*

The group Anonymous is an example of a nonstate actor.

- ◯ True
- ◯ False

Question 26 (1 point) ✓ *Saved*

Which of the following relied on a risk assessment, enabling the use of automated decision making to carefully select weapons based upon the value of the target, the likelihood of detection, and the nature of the target's defenses?

- ◯ FOXACID
- ◯ The Flame
- ◯ Aurora
- ◯ Moonlight Maze

Question 27 (1 point) ✓ *Saved*

Which phase marks the beginning of the intelligence cycle?

- ◯ Processing and Exploitation
- ◯ Analysis and Production
- ◯ Collection
- ◯ Planning and Direction

Question 28 (1 point) ✓ *Saved*

In which of the following attacks does the social engineer create a false set of circumstances and use them to convince the target to take some form of action?

- ◯ pretexting
- ◯ phishing
- ◯ baiting
- ◯ dumpster diving

Question 29 (1 point) ✓ *Saved*

During which phase of the operations security (OPSEC) process is a cost-benefit analysis conducted?

- identification of critical information
- threat analysis
- vulnerability analysis
- risk assessment

Question 30 (1 point) ✓ *Saved*

A vulnerability in a computer system or network that's unknown to the outside world is known as a zero-day vulnerability.

- True
- False

Question 31 (1 point) ✓ *Saved*

Treachery and ruses are not considered a legitimate part of war.

- True
- False

Question 32 (1 point) ✓ *Saved*

In the United States, the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and the Federal Bureau of Investigation (FBI) are responsible for human intelligence (HUMINT).

- True
- False

Question 33 (1 point) ✓ *Saved*

The International Telecommunication Union (ITU), a branch of the United Nations, has engaged in diplomacy by calling on governments to adhere to cyberpeace.

- True
- False

Question 34 (1 point) ✓ *Saved*

Which malware attack targeted Saudi ARAMCO, erasing data on three-quarters of ARAMCO's corporate PCs and replacing the data with images of a burning American flag?

- ◯ Flame
- ◯ Shamoon
- ◯ Aurora Trojan
- ◯ Jester

Question 35 (1 point) ✓ *Saved*

Industrial espionage consists of intelligence activities conducted for national security reasons, rather than for business purposes as its name implies.

- ◯ True
- ◯ False

Question 36 (1 point) ✓ *Saved*

Electronic warfare, a U.S. military information operation, targets inbound attacks, malware, and attackers.

- ◯ True
- ◯ False

Question 37 (1 point) ✓ *Saved*

According to the U.S. Department of Defense's (DoD's) *Information Operations Roadmap*, while all intelligence gathering fits within the domain of information operations, not all intelligence operations are cyberwarfare.

- ◯ True
- ◯ False

Question 38 (1 point) ✓ *Saved*

In which of the following attacks does the attacker send the victim an electronic message in an attempt to solicit sensitive information from the victim?

- ◯ pretexting
- ◯ phishing
- ◯ baiting
- ◯ dumpster diving

Question 39 (1 point) ✓ *Saved*

Which 1998 attack targeted Air Force Base computers, including Andrews Air Force Base in Maryland, the home of Air Force One?

- ◯ Stuxnet
- ◯ Moonlight Maze
- ◯ Solar Sunrise
- ◯ Stakkato

Question 40 (1 point) ✓ *Saved*

The term *the Geneva Conventions* refers to a series of conventions or treaty agreements that deal with the treatment of sick and wounded servicemen, handling prisoners and noncombatants, and the protection of the victims of conflicts.

- ◯ True
- ◯ False

Question 41 (1 point) ✓ *Saved*

Which of the following was launched by China-based attackers, who were against free speech, against Google systems and more than 20 major organizations?

- ◯ Aurora
- ◯ Stuxnet
- ◯ Duqu
- ◯ SQL Slammer

Question 42 (1 point) ✓ *Saved*

The pinnacle of the focused attack is the advanced persistent threat (APT).

- True
- False

Question 43 (1 point) ✓ *Saved*

While the computer network attack (CNA) capabilities of the United States and its allies gives them the ability to intercept communications between commercial data centers operated by Google, the United States and its allies do not have direct access to Google servers.

- True
- False

Question 44 (1 point) ✓ *Saved*

The malicious payload that actually compromises a system that is typically embedded in a more innocuous file is created in which of the following Cyber Kill Chain phases?

- Weaponize
- Deliver
- Install
- Command and Control

Question 45 (1 point) ✓ *Saved*

In the 2000s, which malicious worm infected systems running vulnerable versions of Microsoft SQL Server 2000 database software?

- Code Red
- Stuxnet
- SQL Slammer
- Titan Rain

Question 46 (1 point) ✓ *Saved*

Which decade saw the rise of organized cyberwarfare activities around the world, along with media reports and public debate, and military plans to develop weapons against cyberwarfare?

- 1960s
- 1980s
- 1990s
- 2010s

Question 47 (1 point) ✓ *Saved*

Which of the following was one of the first major attacks against the U.S. cyberinfrastructure, which pointed out to both government leaders and the general public the real risk of cyberattack?

- Solar Sunrise
- Duqu
- Stuxnet
- FOXACID

Question 48 (1 point) ✓ *Saved*

What is PRISM?

- a malicious worm
- a system used by the U.S. government for surveillance of religious organizations
- software used by the U.S. government to gain access to Internet company servers
- a hacking group

Question 49 (1 point) ✓ *Saved*

Who began his social engineering career as a young boy riding the bus system of the San Fernando Valley?

- Kevin Mitnick
- Gary McKinnon
- Kevin Poulsen
- Adrian Lamo

Question 50 (1 point) ✓ *Saved*

A noticeable increase in confidence levels of a bettor after placing a wager from the measurement taken immediately before placing a bet is an example of which of the following?

- social proof
- commitment and consistency
- authority
- scarcity

Question 51 (1 point) ✓ *Saved*

The successful 2011 hacking attack against RSA Security is an example of which of the following types of APT?

- Political agenda
- Corporate espionage
- Activism
- Pacifism

Question 52 (1 point) ✓ *Saved*

A nation-state's sovereignty is the authority to enforce its will in criminal, civil, and administrative procedures within its territory and outside of its territory where allowed by international law.

- True
- False

Question 53 (1 point) ✓ *Saved*

A system under the control of a command-and-control (C2) server is commonly referred to as a botnet.

- True
- False

Question 54 (1 point) ✓ *Saved*

Which of the following is NOT true of the impact of the Internet on the efforts of guerrilla cyberwarriors?

- Can attack nation-states without being present in that country
- Can fundraise from a distance
- The supply chain for combatants is often the same as the one supplying noncombatants, and the guerrilla fighters typically blend into the civilian populace
- Do not have to travel to area where conflict is occurring

Question 55 (1 point) ✓ *Saved*

Which of the following is under U.S. military control?

- U.S. electrical grid
- the Internet
- warfare domains
- e-commerce

Question 56 (1 point) ✓ *Saved*

In April 2007, the Estonian government experienced a series of _____, allegedly in response to moving a war memorial erected by the former Soviet Union. As a result, the Estonian government was forced to dramatically limit communication with the outside world.

- malware infections
- power outages
- embassy bombings
- distributed denial of service (DDoS) attacks

Question 57 (1 point) ✓ *Saved*

In 2008, the hacker named The Analyzer (Ehud Tenenbaum) was arrested and charged with masterminding a series of attacks against financial institutions throughout the United States. He is one of three people responsible for Solar Sunrise.

- True
- False

Question 58 (1 point) ✓ *Saved*

Regarding cyberwarfare, it is often difficult to determine the sources of funding for nonstate actors and whether they are state-sponsored.

- ◯ True
- ◯ False

Question 59 (1 point) ✓ *Saved*

Opportunistic attacks are targeted to a very small, specific group of individuals.

- ◯ True
- ◯ False

Question 60 (1 point) ✓ *Saved*

In _____ warfare, the combatants are typically nation-states that follow the commonly accepted rules of warfare, or those set forth in treaties.

- ◯ conventional
- ◯ unconventional
- ◯ asymmetric
- ◯ total

Question 61 (1 point) ✓ *Saved*

The U.S. Cyber Command (USCYBERCOM) is NOT responsible for _____.

- ◯ Managing cyberspace risk through efforts such as increased training and information assurance
- ◯ Assuring integrity and availability by engaging in partnerships, building collective self defenses, and maintaining a common operating picture
- ◯ Ensuring the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community
- ◯ Conducting operations across on behalf of foreign nonstate actors

Question 62 (1 point) ✓ *Saved*

Omega, a member of the hacking group the Cult of the Dead Cow, first coined the term hacktivism.

- ◯ True
- ◯ False

Question 63 (1 point) ✓ *Saved*

Which of the following is the primary reason an attacker uses a remote access trojan (RAT) and a command-and-control (C2) server as opposed to direct C2 connections to compromised systems?

- ◯ Firewalls prevent a direct connection to the RAT on the compromised system.
- ◯ The IP address of the attacker can be easily obtained on the compromised system.
- ◯ Traffic to the RAT on the compromised system is unencrypted.
- ◯ Demilitarized zones (DMZs) reject all unknown incoming IP address requests.

Question 64 (1 point) ✓ *Saved*

HUMINT operators with the Army use an approach that prioritizes potential sources based upon the likelihood that they will cooperate and the value of the information they possess. Which of the following is NOT one of the three cooperation codes assigned to potential sources?

- ◯ Responds to direct questions
- ◯ Responds hesitatingly to questions
- ◯ Does not comprehend questions
- ◯ Does not respond to questioning

Question 65 (1 point) ✓ *Saved*

The U.S. government has allegedly spied on aid organizations, including the Red Cross.

- ◯ True
- ◯ False

Question 66 (1 point) ✓ *Saved*

_____ have historically been jumping-off points for cyberwarfare attacks because of their significant computing and network resources, and relatively low levels of security.

- ◯ University computer systems
- ◯ Fortune 500 corporations
- ◯ Home computer networks
- ◯ Military computer systems

Question 67 (1 point) ✓ *Saved*

The Tallinn Manual provides a useful framework to understand, interpret, and analyze international law in a cyberwarfare context.

- ◯ True
- ◯ False

Question 68 (1 point) ✓ *Saved*

The role of the terrorist in cyberwarfare is to bring to light those activities that may not survive public scrutiny.

- ◯ True
- ◯ False

Question 69 (1 point) ✓ *Saved*

Cyberwarfare leaders are sometimes centrally coordinated, such as organized crime or nation-state groups, but are also often led by a group or composed of loosely affiliated individuals.

- ◯ True
- ◯ False

Question 70 (1 point) ✓ *Saved*

Many social engineering attacks depend on physical contact to succeed.

- ◯ True
- ◯ False

Question 71 (1 point) ✓ *Saved*

Which stealthy 1998 attack involved reconnaissance and infiltration of computer systems owned and operated by government agencies, universities, and research laboratories located around the

United States?

- Stuxnet
- Moonlight Maze
- Solar Sunrise
- Poison Ivy

Question 72 (1 point) ✓ *Saved*

Which of the following are major criteria for measuring whether force has been used as suggested by the Tallinn Manual?

- The presence of measurable physical damage, the long term effects of the action's results, and the presence of a military character
- The severity of the attack or action, the immediacy of the action's results, and the directness of the action's impact
- The physical harm caused by the attack or action, the long-term effects of the action's results, and the indirectness of the action's impact
- The presence of data destruction, the lack of a military character presence, and the indirectness of the action's impact

Question 73 (1 point) ✓ *Saved*

Which of the following is the right to exercise the functions of a state independently and is a key part of law when applied to cyberoperations and infrastructure?

- jurisdiction
- sovereignty
- control
- responsibility

Question 74 (1 point) ✓ *Saved*

Objective territorial jurisdiction is one of the most difficult concepts to transfer from existing international law into cyberwarfare.

- True
- False

Question 75 (1 point) ✓ *Saved*

The Stuxnet worm is believed to have entered the Natanz, Iran facility through a USB drive carried into the facility unintentionally by an employee.

- ◯ True
- ◯ False

Question 76 (1 point) ✓ *Saved*

Intelligence is the collection, analysis, and dissemination of information about the capabilities, plans, intentions, and operations of an adversary.

- ◯ True
- ◯ False

Question 77 (1 point) ✓ *Saved*

A _____ is best described as a formally recognized country or nation.

- ◯ hacktivist
- ◯ nation-state
- ◯ cyberwarrior
- ◯ combatant

Question 78 (1 point) ✓ *Saved*

_____ warfare is fought with traditional military tactics and weapons, and is often conducted in accordance with international treaties, laws, and agreements.

- ◯ Conventional
- ◯ Unconventional
- ◯ Asymmetric
- ◯ Total

Question 79 (1 point) ✓ *Saved*

Many social engineers combine the liking principle with small gifts that also trigger the need for reciprocity.

- ◯ True
- ◯ False

Question 80 (1 point) ✓ *Saved*

The Syrian Electronic Army (SEA) is the Syrian government's intelligence gathering unit.

- ◯ True
- ◯ False

Question 81 (1 point) ✓ *Saved*

Which of the following are characteristics of an APT?

- ◯ use of denial of service, sophisticated technical tools, and loosely organized
- ◯ highly organized, clear, defined objectives, crude technical tools
- ◯ Sparse financial resources, loosely organized, and loosely defined objectives
- ◯ use of social engineering, clear, defined objectives, and sophisticated technical tools

Question 82 (1 point) ✓ *Saved*

During the operations security (OPSEC) process, the vulnerability analysis phase focuses on indicators, which are friendly actions and information that reveal critical information to the enemy.

- ◯ True
- ◯ False

Question 83 (1 point) ✓ *Saved*

The final phase in the intelligence cycle is Analysis and Production, in which finished intelligence products are delivered to the decision makers who made the requests.

- ◯ True
- ◯ False

Question 84 (1 point) ✓ *Saved*

The U.S. military recognizes the cyber domain as the fifth domain of warfare.

- ◯ True
- ◯ False

Question 85 (1 point) ✓ *Saved*

FOXACID was first released in 2005, has not been updated since 2008, but remains a widely used tool in the hacker community today.

- ◯ True
- ◯ False

Question 86 (1 point) ✓ *Saved*

The Tallinn Manual states that a cyberattack rising to the same level of impact as an armed attack would not qualify as a use of force because it is too difficult to identify the attacker.

- ◯ True
- ◯ False

Question 87 (1 point) ✓ *Saved*

Technical controls can be rendered useless by human actions.

- ◯ True
- ◯ False

Question 88 (1 point) ✓ *Saved*

Which of the following is intended to mislead an enemy without violating the laws of war?

- ◯ espionage
- ◯ fraud
- ◯ treachery
- ◯ ruse

Question 89 (1 point) ✓ *Saved*

In total cyberwarfare, there are no commonly agreed-to limits on cyberwar activities.

- ◯ True
- ◯ False

Question 90 (1 point) ✓ *Saved*

Encrypted connections make it extremely difficult to detect command-and-control connections on a network.

- ◯ True
- ◯ False

Question 91 (1 point) ✓ *Saved*

Script kiddies are individuals who discover vulnerabilities and then write scripts to exploit the newly discovered vulnerabilities.

- ◯ True
- ◯ False

Question 92 (1 point) ✓ *Saved*

Which of the following is NOT a typical characteristic of successful solo hackers and small groups of activist cyberwarriors?

- ◯ Target governments and the military rather than corporations
- ◯ Persistence
- ◯ Highly motivated
- ◯ Highly skilled

Question 93 (1 point) ✓ *Saved*

Which U.S. military information operation targets social media, Web sites, e-mail, and other communications that influence targets?

- ◯ intelligence gathering
- ◯ electronic warfare
- ◯ psychological operations
- ◯ operations security

Question 94 (1 point) ✓ *Saved*

Which intelligence discipline is most likely to include the use of cryptanalysis?

- ◯ open source intelligence (OSINT)
- ◯ human intelligence (HUMINT)
- ◯ signals intelligence (SIGINT)
- ◯ geospatial intelligence (GEOINT)

Question 95 (1 point) ✓ *Saved*

The purpose of the Hague Conventions was to address treatment of victims of cyberwarfare.

- ◯ True
- ◯ False

Question 96 (1 point) ✓ *Saved*

Spear phishing is an example of an opportunistic attack.

- ◯ True
- ◯ False

Question 97 (1 point) ✓ *Saved*

During which phase of the intelligence cycle is raw data converted to a usable form and data is translated from one language to another, if necessary?

- ◯ Planning and Direction
- ◯ Collection
- ◯ Processing and Exploitation
- ◯ Analysis and Production
- ◯ Dissemination

Question 98 (1 point) ✓ *Saved*

Law enforcement officers, judges, and tax collectors all operate under which of the following type of authority?

- ◯ international
- ◯ legal
- ◯ federal
- ◯ social

Question 99 (1 point) ✓ *Saved*

In 1971, the United States Supreme Court ruled in the case of *New York Times Co. v. United States* that the Pentagon Papers could continue to be published freely.

- ◯ True
- ◯ False

Question 100 (1 point) ✓ *Saved*

What are the primary ways in which corporations become involved in cyberwarfare?

- ◯ Infecting competitors with ransomware and cooperating with organized crime
- ◯ Being vocal critics of cyberwarfare activities and industrial espionage
- ◯ Industrial espionage and cooperating with intelligence agencies
- ◯ As targets of diplomatic organizations and in magnifying the effects of cyberwarfare in the media

---

Submit Quiz *100 of 100 questions saved*