The Common Criteria make up an international standard for computer security certification and testing.

True

Which of the following is a common defensive device found in defense-in-depth designs?

intrusion prevention system (IPS)

Which of the following provides standards and a technical framework from the National Security Agency?

Information Assurance Directorate (IAD)

When considering C-I-A in the context of defense in depth, which of the following is true?

The more you protect confidentiality, the harder it becomes to provide provable integrity.

System administrator privileges are one of the most heavily protected and monitored assets in any successful defense-in-depth design.

True

DoD Instruction 8500.01E specifically addresses defense in depth.

False

In traditional information security operations, security professionals can guarantee their employers that there are many ways to be perfectly secure.

False

Security policies and procedures are found in which layer of the US-CERT's defense-in-depth strategy?

network

security risk

operational

host

Device integrity helps to ensure that attackers have not modified or changed systems and devices.

False

The concept of providing defense in depth by layering protective capabilities has been in use for thousands of years.

True

Layered defenses make it more likely that a single attack can completely compromise a network or system.

False

The National Security Agency's (NSA's) people-based strategy is based on a framework that includes which of the following?

policies and procedures, training and awareness, and system administration

Some of the biggest problems with defense in depth result from tradeoffs it creates simply because of the way it must be implemented.

True

When designing defense in depth, which of the following is one of the hardest challenges to defend against?

technological change

The term self-replicating network (self-defending network) implies that the network is able to respond to attacks by changing rules, modifying how it is configured, and otherwise responding to problems.

False

Which of the following ensures that information has not been modified by unauthorized users or systems, and remains accurate and consistent?

integrity

Defense in depth has disadvantages for those who are defending a network because complex, more expensive defenses are required in each layer.

False

Which of the following is the ability to validate that the system or user is who he or she claims to be?

authentication

Which of the following could result during an attack when there isn't sufficient internal defense?

The attackers can pivot, attacking other systems.

Which of the following areas of the National Security Agency's (NSA's) Information Assurance and defense in-depth conceptual model emphasizes the need to defend in multiple places at once?

technology-based strategy

Authentication codes are cryptographic functions that take a block of data and perform operations on it to produce a fixed-length string of characters. (Hashes)

False

Self-defending systems are intended to adapt to prevent attacks by monitoring systems, users, and network traffic.

True

Unlike traditional warfare, cyberwarfare is fought only defensively.

False

The National Security Agency's Information Assurance Directorate (IAD) provides an extensive, detailed guide intended to provide guidance on how to counter attacks by non-nation-states.

False

Defense in depth is the idea that defenses should have more than a single layer of protection between an attacker and the protected systems, data, or networks.

True

Which of the following best describes dynamic defense?

Defense that can change in reaction to threats and new risks

Which of the following is true of endpoints, such as laptops, tablets, and mobile devices?

Security for these devices can be incredibly complex due to the wide variety of devices.

A certificate authority that issues and verifies certificates is part of which of the following?

public key infrastructure (PKI)

Which of the following best describes a network enclave?

A separated portion of a network that isolates systems based on rules or purpose

Many of the controls on the SANS Top 20 Critical Security Controls list match those on the National Security Agency's Information Assurance Directorate (IAD) list.

False

Key management and public key infrastructure are a part of which of the following strategy?

encryption

Damage containment ensures that credentials are not exposed or misused.

True

DoD Instruction 8500.01E requires which of the following?

The ability of technology components to self-defend and optimize with minimal human intervention

The daily activities of a defense-in-depth strategy occur in the technology portion of the National Security Agency's defense-in-depth conceptual model.

False

Which of the following is the first step in computer network defense (CND) strategies?

Identifying the likely attackers

The National Security Agency (NSA) C-I-A triad consists of which of the following principles?

confidentiality, integrity, and availability

Which of the following best describes application whitelisting?

A technological solution that uses known, allowed programs to run on trusted systems

The US-CERT's defense-in-depth strategy for protecting individual systems against a sample attack contains which of the following layers?

administrative, security risk, and physical

The Department of the Navy computer network defense (CND) defense-in-depth strategy combines elements at the host, network, network edge, and policy layer.

True

Using technological factors to attack systems was an important part of the Stuxnet malware attack on Iranian nuclear facilities.

False

Symmetric ciphers rely on which of the following?

a shared key

Which of the following best describes cryptography?

The study and practice of techniques for secure communication that is protected from adversaries

Which of the following relies on key pairs with a public and a private key used in the encryption algorithm?

asymmetric encryption

The broad use of cryptography in its many forms is a key part of cyberwarfare.

True

Which of the following best describes a substitution cipher?

Each letter of the alphabet is replaced by the specific frequency of the characters.

The Enigma devices originally used by the Germans used eight wheels to perform complex substitutions of letters very much like a series of Caesar ciphers.

False

Which of the following is true of quantum cryptography?

Quantum cryptography would change the role of encryption and cryptanalysis in cyberwar.

Which of the following is the main goal of cryptography?

To protect communication from adversaries

Nonrepudiation means that the sender cannot claim that someone falsely sent the message posing as the sender.

True

Public key encryption provides only confidentiality and authentication.

False

Which of the following is true about symmetric encryption?

Symmetric encryption is relatively fast compared with asymmetric encryption.

Zeus is a fast-spreading macro virus that is distributed as an e-mail attachment that disables a number of safeguards in Microsoft Word when the attachment is opened.

False

Hashes take a message and generate a unique output value based on the message.

True

Hashing algorithms are vulnerable to attacks that create collisions.

True

Brute-force attacks are sometimes called passive attacks.

False

To date, Data Encryption Standard (DES) has not been broken.

False

Which of the following best describes the effect a meet-in-the-middle attack has on cryptosystems?

The expected protection provided by a cryptosystem is far less than expected.

Which of the following is a cryptographic system that substitutes values or words for other words?

Code

What is one of the best ways to attack encryption?

Acquire the keys.

The U.S. Department of Defense (DoD) uses a key fob for identification of both military and civilian staff.

False

What are the consequences when a user who is unfamiliar with asymmetric key systems accidentally sends the private key to someone they want to communicate with?

A new key pair must be generated key.

Defenders use encryption to protect data at rest and during transit.

True

The U.S. government defines how cryptographic modules are accredited for modern cryptosystems in which of the following?

Federal Information Processing Standard (FIPS) 140-2

Which of the following best describes steganography?

The practice of concealing a message inside another message

Which of the following accurately describes Kerckhoffs's principle?

A cryptographic system should remain secure even if the enemy knows everything about the system except the key.

Advanced Encryption Standard (AES) allows which of the following three key strengths?

128 bits, 192 bits, and 256 bits

The first place that attacks occur against the modern encryption system is while the data is in use and unencrypted.

True

Asymmetric encryption relies on key pairs.

True

Modern cryptographic systems are far less complex than early cryptographic systems.

False

Steganography is limited to hiding text in images.

False

Which of the following is a common technique to make applications that use hashes for storing passwords more secure?

salting

Which of the following uses strong RSA encryption to extort money from infected users?

Cryptolocker malware

Key-handling practices for asymmetric encryption systems are critically important.

True

Drive encryption is vulnerable to an attack in which the user is persuaded to provide his password. What is this type of attack?

social engineering

Attacks against cryptographic systems are known as ____________.

cryptanalysis

Symmetric ciphers do not rely on a shared key.

False

Modern malware can use encryption by encrypting the malware itself when on disk and running on systems.

True

Cryptography is the study and practice of maintaining and assuring the accuracy of data.

False

Codes are intended to provide confidentiality and message integrity.

False

Which of the following is a common solution for future defenses against attacks on encryption?

Increased key length for existing strong encryption algorithms

The concept of defense in depth is not important when deploying endpoint defenses.

False

Which of the following combines both aggressor and defender teams?

purple team

When traditional security measures have been put in place, a single flaw open to exploit cannot provide the way in for an attacker.

False

Which of the following U.S. Department of Defense (DoD) initiatives is a broad array of systems that provides situational awareness and can react and respond?

Command, Control, Communications, Computers, and Intelligence (C4I)

Targeting endpoint systems is an attractive option for attackers.

True

The use of anti-malware requires that staff know about threats and attacks.

False

Vulnerability scanning uses attacks and exploits against an organization to verify the effectiveness of its security controls.

True

The term military systems describes a range of devices and platforms.

True

Due to a push by the Food and Drug Administration (FDA), many standards for the security of medical devices have been created and adopted.

False

A Trusted Platform Module (TPM) chip is a cryptographic processor built in to the motherboard of the device.

True

Due to their critical role in battlefield control, programmable logic controllers (PLCs) are an important part of current and future combat strategies.

False

Traditional techniques for detecting malware have become more effective over the past decade.

False

The U.S. Wounded Warrior design includes individual solider computer systems that provided monitoring of individual soldiers with health sensors.

False

Cyberhygiene is a term that defines security practices limited to endpoints.

False

Global positioning system (GPS) attacks against U.S. drones have allegedly caused the drones to attempt landing in the wrong place. This is an example of which type of attack?

Attacks that use the endpoint's normal function against it

Distributed database systems (DDSs) are frequently used to control water and wastewater treatment.

False

Which of the following best describes policies?

Policies assign responsibility and set the overall tone for computer network defense activities.

Which of the following incidents demonstrates that the boundaries of cyberwarfare may include direct physical harm?

The Stuxnet worm infected at least 14 industrial sites in Iran, allowing the attackers to spy on the industrial systems.

Which of the following is the reason drone software and the systems used to control them are a target of attacks on drone platforms?

Drone command-and-control system links are encrypted.

Blacklisting builds a list of prohibited applications, files, sites, or other data or access.

True

The Aurora malware was specifically designed to attack the Siemens Simatic S7-300 PLC's firmware.

False

The most common type of endpoint from a cybersecurity perspective is the mobile phone.

False

Organizations such as the U.S. government's U.S. Computer Emergency Readiness Team (US-CERT) provide which of the following?

information sharing

When specific accesses must be blocked, or when the list of known files is already established, which of the following is most effective?

blacklisting

Most disk encryption systems that aren't built in to the disk itself are vulnerable to which of the following attacks?

side-channel

The root of most defensive strategies is a cyberdefense policy.

True

What percentage of military aircraft functions in recently developed models are handled by software?

80

Which of the following is a sensor that provides reporting back to the central data collection system in Supervisory Control and Data Acquisition Systems (SCADA) systems?

remote telemetry unit

Which of the following is the main reason industrial control systems (ICSs) are often not as well secured as a traditional computing infrastructure?

ICS systems have high requirements for stability and continuous operations.

An industrial control system (ICS) includes the devices and systems that control industrial production and operation.

True

Which of the following is the primary reason personal computers provide attackers with a multitude of attack options?

Because the software personal computers run is usually commercially available.

The typical layers of defense for a computer workstation start at which level?

firmware level

Which of the following is part of the U.S. Department of Defense's (DoD's) process to provide a defensive endpoint strategy?

Utilize existing defense operating concepts and computing architectures.

Embedded systems create unique challenges for defenders because security standards are rare or nonexistent for most embedded systems.

True

Security standards define the settings and options a system, application, or other part of an endpoint system has in place.

False

Which of the following is an example of firmware?

software that operates a pacemaker

Which of the following includes awareness on the part of individuals in the U.S. Department of Defense (DoD), software and operating system updates, cybersecurity practices for users and administrators, and configuration management? It is critical to the DoD's cyberspace operations endpoint strategy.

cyberhygiene

Many of the most successful attacks against endpoints in cyberwar have been _______ based.

malware

The U.S. Future Force Warrior design provided monitoring of individual soldiers with _______.

advanced cyberwarfare tools

Which of the following best describes the role of central management systems?

They are used to make changes and updates to systems from a single, central location.

Which of the following provides the ability to inspect the actual protocols and application traffic that flow through a firewall?

application-aware firewall

In the National Institute of Standards and Technology's (NIST's) use of network security boundaries, which of the following provides separation between two networks while allowing controlled traffic to pass between them?

the subsystem guard

The U.S. Defense Information Assurance Certification and Accreditation Process (DIACAP) provides multiple levels of IP network services based on the data classification the network transmits.

False

The move to the U.S. Department of Defense (DoD) risk management framework (RMF) for information technology (IT) better aligns the department with other U.S. government agencies.

False

The U.S. Department of Defense (DoD) uses seven mission assurance levels, known as Mission Discretionary Control (MDC) levels.

False

Which of the following attacks can allow attackers to send traffic to other virtual local area networks (VLANs)?

Question 6 options:

VLAN hopping attacks

Which of the following best describes an active defense?

A network that adapts to attacks

Cyberwarfare defenders only need to consider local area networks (LANs) when they design defenses.

False

Secure Sockets Layer (SSL) is the standard of choice for secure Web traffic because Transport Layer Security (TLS) is now outmoded.

False

In cyberwarfare operations, which of the following is the process by which systems and networks are kept online and functioning?

Mission assurance

Which of the following best describes advantage of the Onion Router (TOR)?

Provides anonymity to TOR users

Active defenses require a carefully constructed network and provide many challenges for defenders.

True

The U.S. Department of Defense (DoD) pays particular attention to the concept of mission assurance.

True

Which of the following is the global telecommunications network for the U.S. military operated by the Defense Information Systems Agency (DISA)?

Defense Information Systems Network (DISN)

Networks rely on routers to send data between computer networks.

True

Device acquisition policies and procedures are increasingly less important in computer network defense.

False

A honeypot relies on the fact that unused space should have no legitimate traffic sent to it.

False

Network protocols are used to determine how traffic flows between and inside networks, how traffic errors are handled, and a huge variety of network functions.

True

Which of the following is a protocol used between network routers to communicate information about how and where to send traffic?

Border Gateway Protocol (BGP)

Using multiple service providers when commercial services are used to provide network connectivity is an aspect of which of the following?

Providing a resilient network

The technology portion of the National Security Agency's (NSA's) defense-in-depth strategy relies on which of the following?

an analyze, mitigate, resolve model

An acceptable use policy (AUP) provides information on what systems or network IP addresses are allowed to pass through a router.

False

Which of the following is the reason the term darknet is sometimes applied to TOR networks?

Darknets operate in a difficult-to-detect part of the Internet.

Which of the following is true regarding access control lists (ACLs)?

They provide less-advanced features than the more-advanced types of firewalls.

Intrusion detection systems (IDSs) or devices were created to prevent attacks based on distinct allowed applications.

False

The need for mission assurance and the ability to react mean that surviving network attacks is an important part of defending networks in cyberwar.

True

The technology portion of the National Security Agency's (NSA's) People/Technology/Operations defense-in-depth strategy relies on a Protect, Defend, React paradigm.

False

A well-designed firewall's final rule will always be a rule that allows all traffic not specified in prior rules to pass through it.

False

The network border is often the last line of defense in cyberwar.

False

Which of the following is designed to provide a transport network for data falling under the U.S. government's Secret classification?

Secret IP Data

The Stuxnet attack succeeded due to which of the following?

Contracted engineers who used USB flash drives to transfer data between systems

Security Event Managers (SEMs) help to sort through the massive amounts of data that a well-configured and logged network provides.

False

Which of the following is the primary reason the U.S. Department of Defense's (DoD's) mission assurance strategy creates a challenge for intrusion prevention system (IPS) operators?

It increases the risk of network outages

Mission assurance requires additional effort in which of the following areas?

Design, maintenance, and management of computer and other networks

One of the most common ways to physically separate networks is using a virtual LAN (VLAN).

False

Which of the following is a defense strategy for the placement of virtual private network (VPN) users?

Place in a distinct zone with different monitoring rules

Which of the following are the four major types of networks most commonly found in organizations?

local area networks (LANs), wide area networks (WANs), the Internet, and proprietary networks

Access to the physical cables that data travels over is harder to prevent than implementing physical security boundaries like walls.

True

Which of the following is the code name the National Security Agency (NSA) uses for technologies related to both capturing and protecting information from capture through the use of leaked emanations?

Tempest

Which of the following best describes an active response?

Hacking the hacker

Which of the following models is often written as "no write down, no read up"?

Bell-LaPadula

Magnetic media can be erased using a tool known as a decoder, which uses very strong magnetic fields to wipe the media.

False

Data analysis tools monitor network traffic and transfers to removable media to stop the transfer of sensitive data.

False

Which of the following is affected when an attacker changes data?

data availability

Having more than one server providing a service is an example of which of the following?

redundancy

Ensuring proper backups are performed is an example of providing data integrity.

False

Software tools that prevent data from being shifted to another format by preventing printing, screenshots, or other access are an example of which of the following?

digital rights management (DRM)

Additional file data that includes the creator of a file, when it was created, and the data classification is referred to which of the following?

metadata

All encryption algorithms have very long life spans and can go for a minimum of 50 years without the discovery of flaws.

False

Solid state drives can be securely wiped using the same drive-wiping software that is used on hard disk drives.

True

The additional information contained in a file that describes the data is known as an alternate data stream.

False

Which of the following is the process of labeling data based on its sensitivity and handling requirements?

data classification

Data that has been removed from its classification scheme is declassified.

True

Despite the best efforts of defenders, even strong encryption systems can be defeated in which of the following scenarios?

Users move the protected data outside the protective system

Which of the following is affected when distributed denial of service (DDoS) attacks are executed?

data availability

Data loss prevention (DLP) can require significant amounts of maintenance.

True

The use of policy to manage the life cycle and flow of data through an organization is known as Data Lifecycle Management (DLM).

False

Which of the following has made it possible for organizations to continue to provide services despite large-scale attacks?

The use of cloud services

A common rule of thumb is that the physical location of backups and other disaster recovery systems be at least how far apart?

90 miles

Which of the following is an often-forgotten data exposure risk for many organizations?

desktop printer

Encryption is particularly effective when data is in use.

False

The use of policy to manage the life cycle and flow of data through an organization is known as which of the following?

Data Lifecycle Management (DLM)

The U.S. government has historically had as many as 1,000 different designations for data.

False

Which of the following is a step in the National Security Agency's (NSA's) typical response process to data loss?

Isolate the compromised system(s) to limit the chance for further damage.

Government agencies use data warehousing to label data based on its need for secrecy and the handling requirements that it requires.

False

Which of the following is used to find sensitive information in file stores, workstations, servers, and other network locations?

discovery data loss prevention (DLP) systems

The Bell-LaPadula security model protects integrity by preventing high-security-level users from reading lower-level data and lower levels from writing upward.

False

Data that has had its classification level lowered, but that remains classified, is known as which of the following?

Downgraded

The increasing use of virtualization has allowed organizations to create redundancy.

True

Which of the following is often encrypted to protect data in case the data storage media is stolen or otherwise exposed?

data at rest

Defensive operations in cyberwar often have a strong focus on protecting data that is stored on workstations, devices, and in network file storage.

True

Data integrity is commonly checked using a cryptographic hash function.

True

Which of the following is expected to have at least a 10-year life span but may last as long as 50 years if stored properly?

magnetic media

If data must remain secure for more than a decade, current encryption is likely to be significantly less protective than it was when the file or drive was first encrypted.

True

Network-based data loss prevention (DLP) systems are installed on individual workstations and devices.

False

Digital rights management (DRM) software can be used to help control how and where labeled data and programs are used.

True

Which of the following is a critical control recommended by the National Security Agency (NSA) to combat data spills?

Creation and enforcement of data protection policies

To prevent a nation-state-backed organization from recovering data on discarded hard drives, which of the following is necessary?

Using a secure hard drive destruction service

Which of the following is true about data loss prevention (DLP) systems?

DLP systems can't be expected to stop all data loss.

Data spillage occurs when classified or sensitive data is transferred to unauthorized or unaccredited systems, individuals, or applications.

True

Question Chapter 14

According to Army Field Manual 3-0: Operation, which principle of war requires that the attack take place in a time or place where the enemy can't immediately react in an effective manner?

Surprise

At the tactical level of warfare, broad goals are set by senior political and military officials, including the president, secretary of defense, and commander of the Joint Chiefs of Staff.

True

The participants in irregular warfare may include nonstate actors.

True

According to the Joint Chiefs of Staff "Principles of Joint Operations," which principle states that military commanders must take measures to ensure that the commitment exists to achieve the desired end state?

Perseverance

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

True

According to Army Field Manual 3-0: Operation, which principle of war states that the more complex or ambiguous a set of orders, the more likely it is that the unit will fail to achieve its objective?

Simplicity

According to Army Field Manual 3-0: Operation, which principle of war states that military commanders should concentrate their combat forces at the decisive time and location?

Mass

The U.S. military has discarded the term "conventional warfare" because it was widely used during the cold war to refer to non-nuclear warfare.

True

According to U.S. military doctrine, war is socially sanctioned violence to achieve a political purpose.

True

Each U.S. military unit has its own cyberwarfare component. The actions of these components are coordinated by the _________.

U.S. Cyber Command (USCYBERCOM)

According to Army Field Manual 3-0: Operation, which principle of war states that every military action must have a clearly defined purpose?

Objective

Although the U.S. Army embraces the nine principles of war, the U.S. Joint Chiefs of Staff use a different list, known as the Principles of Joint Operations.

True

In U.S. military doctrine, traditional warfare is defined as "characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)."

False

The U.S. Marine Corps is engaged in operations that cross between the land and sea domains of warfare.

True

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

True

According to Army Field Manual 3-0: Operation, which principle of war states that a single commander should be responsible for achieving each military objective?

Unity of command

The Chinese general Sun Tzu wrote "Joint Cyberspace Operations," a treatise on military doctrine that outlined basic strategies that every military commander should follow.

False

According to Army Field Manual 3-0: Operation, which principle of war ensures that operations at lower levels are consistent with the higher-level commander's intent?

Objective

Which military unit is responsible for cyberwarfare defense functions?

All forces

What are the three levels of warfare?

strategic, tactical, and operational

A U.S. military commander that orders a Navy Seal team to invade a specific location to apprehend a terrorist is an example of the ______ level of warfare.

tactical

According to Army Field Manual 3-0: Operation, which principle of war states that military commanders must seize, retain, and exploit the initiative?

Offensive

The Surprise principle of war requires a completely unaware enemy.

False

According to the Joint Chiefs of Staff "Principles of Joint Operations," the Legitimacy principle focuses on _________.

consistency with national laws, and international treaties and obligations

Currently, U.S. military doctrine separates warfare into _____ forms.

traditional versus irregular

The USCYBERCOM emblem contains a string of characters that is the MD5 hash of the command's mission statement.

True

The principles of warfare and joint operations form the core of military doctrine

True

According to the Joint Chiefs of Staff "Principles of Joint Operations," which principle states that, while conducting military operations, commanders should limit collateral damage and prevent the unnecessary use of force?

Restraint

Which of the following is NOT one of the U.S. Department of Defense's (DoD's) five pillars of cyberwarfare?

Increase offensive cyberwarfare efforts

Cyberwarfare operations may take place at any level of warfare: strategic, operational, or tactical.

True

At the operational level of warfare, commanders set the objectives for military campaigns and major operations.

True

Which of the following is NOT true of the U.S. Strategic Command (USSTRATCOM)?

Is responsible for providing unbiased assessments of the Department of Defense's cyberwarfare efforts

According to Army Field Manual 3-0: Operation, which principle of war states that commanders must never allow enemy forces to gain an advantage; this is essential to preserving and protecting a military's power?

Security

The levels of warfare are in this order: strategic, tactical, and operational.

False

The strategic level of warfare addresses the national-level objectives of the war.

True

According to Army Field Manual 3-0: Operation, which principle of war keeps enemy troops at a disadvantage by forcing them to deal with new problems and dangers faster than they can react to the changing dynamics of the battlefield?

Maneuver

Responsibilities for U.S. military operations are divided between the individual military services and joint commands. Services are responsible for training and equipping troops, whereas joint commands fight wars through combatant commanders.

True

Which of the following is NOT true of doctrine?

It provides detailed plans for all types of military operations.

Nation-states may engage in both traditional and irregular warfare. The U.S. military engagements since September 11, 2001, have been primarily irregular in nature.

True

The principles of war are not consistent from nation to nation.

True

Question chapter 15

Switches connected to the public Internet often block more than half of the traffic that is sent to systems behind them.

False

Which of the following does not pose a constant threat to organizational resources?

security policies

U.S. government estimates put the losses due to stolen intellectual property (IP) at $30 million a year.

False

In many cases, the U.S. government requires ________ as a means of verifying cyber defense proficiency.

certification

Cyberspace is typically more hospitable to defenders than attackers.

False

Defenders who find advanced malware on their systems and networks often attempt to reverse engineer it to identify the attackers, as well as what the malware can do.

True

Which of the following is a partnership between the FBI and the private sector that shares information and intelligence to prevent attacks. The partnership works with 16 critical sectors, including the chemical, communications, manufacturing, defense/industrial, and transportation systems sectors.

Infragard

The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) is responsible for the creation of the Tallinn Manual.

True

Cyber defenders typically advance faster than cyber attackers.

False

The Control System Security Center (CSSC) is a joint effort spearheaded in _______ to improve the security of control systems for infrastructure.

Japan

Cyberwar tools that can attack countries far away from the originating country's borders are much easier to create and to obtain than traditional kinetic weapons that could reach similar distances. This means that cyberwar weapons are more accessible to countries that want to develop an offensive cyberwar capability.

True

Which of the following is an information security company that has worked extensively with advanced persistent threat (APT) research and incident response?

Mandiant

International law in the form of the Geneva Conventions and numerous other treaties has not yet been updated to accommodate the new ways in which international cyberwar affects both military targets and civilian infrastructure and populations.

True

A typical network can see thousands or even tens of thousands of malicious network scans a day.

False

In the future, exploit code is likely to become more complex to make it even more difficult to determine the creator's identity.

False

Information that links attacks can be a great help in determining who may have written the malware and chosen its targets.

True

Which of the following is NOT an expected result as cyberwarfare activities increase?

fewer hacking schools

What term refers to the electronic interconnection of computers, mobile devices, medical devices, vehicles, household appliances, wearable computers, and so on?

Internet of Things

Commanders do not always understand the cyber-risks they face.

True

What is cryptocurrency?

a difficult-to-track payment method

Although cyberattacks are on the increase, military cybersecurity jobs are not expected to grow in numbers over the next few years due to budget restrictions.

False

Which of the following is NOT a reason why it's possible for nonstate actors to conduct complex attacks like Stuxnet?

Intelligence gathering is not difficult.

Which of the following is NOT a cyberwar legal issue that experts are expected to consider in the near future?

The requirement to respect other nations' territorial sovereignty and jurisdictional rights

Which of the following is NOT a typical phase of the advanced persistent threat (APT) life cycle?

Cleanup

Widely used smaller attacks are much less effective than a single attack in one facility with a major impact.

False

Attackers who seek to retain long-term access to gain intelligence and to control infrastructure and systems, along with the tools they use, are known as ________________.

advanced persistent threats (APTs)

The term netwar describes a new information-related conflict that tries to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it.

True

Which of the following is NOT a typical technique for determining the source of an attack?

Strengthen the security of the victim network.

The ability to conduct attacks using massive computer systems is also easily attainable for both nation-states and nonstate actors.

True

As the attack methods and advanced exploit tools and techniques used by nation-states become available to cybercriminals, insurrectionists, and individuals, it will become increasingly difficult to determine if an aggressor is a traditional nation-state opponent or a group that doesn't abide by the traditional and accepted rules of war.

True

Because an opponent can hide a cyberattack's ________, nation-states might use analysis of cyberattacks to determine which adversary conducted them.

source

What factors, more than any others, make the ability to conduct attacks using massive computer systems attainable to nation-states and nonstate actors?

cloud computing and cryptocurrency

Nation-state resources are required to duplicate a complex attack like Stuxnet.

False

The U.S. legacy information architecture and some weapons systems are not designed to be robust and to survive in a hostile cyber environment.

True

Future cyberwarriors will continue to use long-term attacks to acquire and maintain access to government and civilian systems, both to provide intelligence information and to _______________.

gain a competitive advantage for business

Which of the following is NOT an expected security countermeasure for network-attached vehicles of the future?

demilitarized zone

The FBI maintains a Cyber Most Wanted list.

True

Which of the following is a test attack environment that helps students prepare for defending against cyberattacks in the real world?

SANS NetWars CyberCity

Which U.S. government entity ensures cloud computing service providers meet security standards?

Federal Risk and Authorization Management Program (FedRAMP)

Which of the following is NOT true of Sun Kailiang?

Chinese state media retaliated by accusing Westinghouse and SolarWorld of helping the NSA perform international intelligence-gathering.