Group 6
Information Warfare

1. Defined by Merriam-Webster as "the use of spies to learn about the intentions and operations, particularly of a foreign government or a rival firm."
   A. Espionage
   B. Information Warfare
   C. Cyber Pornography
   D. Big Data

2. It is defined as “action taken to achieve information superiority by affecting an adversary information, information-based processes, information systems and computer-based networks while defending one’s own information, information-based processes, information systems and computer-based networks.
   A. Data Analysis
   B. Psychological Warfare
   C. Information Warfare
   D. Information Welfare

3. Cybercriminals leverage an unknown security vulnerability or software flaw prior to discovery and patching by the software developer or the customer’s IT team.
   A. Four-day exploitation and intrusion activity
   B. Three-day exploits
   C. One-day exploits
   D. Zero-day exploits

4. It refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
   A. Hacker Warfare
   B. Human Intelligence
   C. Signals Intelligence
   D. Command and Control Warfare

5. It is also referred to as photo intelligence. One of the earliest forms of imagery intelligence took place during the Civil War, when soldiers were sent up in balloons to gather intelligence about their surroundings.
   A. Open-source intelligence
   B. Human Intelligence
   C. Measurement and Signatures Intelligence
   D. Imagery Intelligence

6. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.
   A. Command and Control Warfare
   B. Economic Information Warfare
   C. Cyberwarfare
   D. Intelligence-based Warfare

7. It is intelligence about weapons and equipment used by the armed forces of foreign nations (often referred to as foreign material).
   A. Cyber Intelligence
   B. Technical Intelligence
   C. Financial Intelligence
   D. All of the above

8. It is a technical branch of intelligence gathering which serves to detect, track, identify or describe the signature (distinctive characteristics) of fixed or dynamic target sources.
   A. Geospatial Intelligence
   B. Measurement and Signature Intelligence
   C. Open-source Intelligence
   D. Signals Intelligence

9. It is collecting information about a particular entity for the benefit of another using more than one interrelated source.
   A. Hacker Warfare
   B. Cyber Espionage
   C. Intelligence Gathering
   D. Data Gathering and Procedures

10. There are different intelligence gathering disciplines, **EXCEPT** one.
   A. Digital Network Intelligence
   B. Financial Intelligence
   C. Geospatial Intelligence
   D. Universal and Operations Intelligence

11. It is the gathering of information about the financial affairs of entities of interest, to understand their nature and capabilities, and predict their intentions. Generally, the term applies in the context of law enforcement and related activities.
   A. Banking Intelligence
   B. Financial Intelligence
   C. Forensic Intelligence
   D. Photographic Intelligence

12. A cyber espionage group which could potentially be behind the attacks called APT32 and APT-C-00 in Vietnam.
   A. Slingshot APT
   B. WannaCry
   C. I Love You
   D. OceanLotus

13. There are different types of Information Warfare, EXCEPT one:
   A. Information Manipulation
   B. Cyber Warfare
   C. Economic Information Warfare
   D. Psychological Warfare

14. A threat actor convinces an employee or a contractor to share or sell information or access to the system to unauthorized users.
   A. Outside Source
   B. Watering holes
   C. Inside Source
   D. Inside Actors

15. Malicious actors can infect legitimate websites commonly visited by the victim or people associated with the target with malware for the explicit purpose of compromising the user.
   A. Phishing
   B. Vishing
   C. Watering hole
   D. Spear-phishing

16. A hacker targets specific individuals with fraudulent emails, texts, and phone calls in order to steal login credentials or other sensitive information.
    A. Malware
    B. Spear-phishing
    C. Worms
    D. Virus

17. All three techniques are means to the same general end – preventing the enemy from getting complete, correct information. Because of their similarity, many of the same weapons are used to achieve one or more of the goals.
    A. Information Manipulation, Privacy, and Integration
    B. Information Denial, Control, and Distribution
    C. Information Disturbance, Degradation, and Denial
    D. Information Protection, Distribution, and Integration

18. In the context of information warfare is the alteration of information with intent to distort the opponent's picture of reality.
    A. Information Manipulation
    B. Information Denial
    C. Information Disturbance
    D. Information Transport

19. May also be perpetrated by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, seeking to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national security, economic competitiveness, and/or military strength.
    A. Cybersecurity
    B. Cyber Espionage
    C. Cybersex
    D. Cyber Mining

20. One of the most broadly agreed upon aspects of information warfare is the need to minimize the amount of information to which your opponent has access. A large part of this is protecting the information you have from capture by the other side.
    A. Information viability
    B. Information availability
    C. Information transparency
    D. Information protection

21. Cyber spies most commonly attempt to access the following assets EXCEPT one.
    A. Your printer
    B. Academic research data
    C. Military intelligence
    D. IP, such as product formulas or blueprints

22. There are different intelligence gathering methods EXCEPT one.
    A. Interception of telecommunications
    B. Transmission reproduction
    C. Module writing and distribution
    D. On-site audio monitoring

23. Intelligence gathering plays a major role in today's warfare as intelligence provides us with knowledge about what the enemy may be doing or is going to do in the future.
    A. True
    B. False. Cyber espionage plays a major role in today's warfare as intelligence provides us with knowledge about what the enemy may be doing or is going to do in the future.

24. Information Warfare is a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent.
    A. True
    B. False. Geospatial Intelligence is a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent.

25. It is reported that Thailand has an army of more than 6,000 hackers that raise money to pay for the country's nuclear program. They have a recent attack that has been attributed to them and it is APT37.
    A. True
    B. False. It is reported that North Korea has an army of more than 6,000 hackers that raise money to pay for the country's nuclear program. They have a recent attack that has been attributed to them and it is APT37.

26. Measurement and Signatures Intelligence includes the advanced processing and use of data gathered from overhead and airborne imagery intelligence and signals intelligence collection systems.
    A. True
    B. False. Open-source Intelligence includes the advanced processing and use of data gathered from overhead and airborne imagery intelligence and signals intelligence collection systems.

27. Digital Network Intelligence is gathered from cyberspace or interconnected technology.
    A. True
    B. False. Technical Intelligence is gathered from cyberspace or interconnected technology.

28. The root of the ethical problem over the collection of educational materials lies in the need to overcome the determined will of the person with the secret not to allow it to be known.
    A. True
    B. False. The root of the ethical problem over the collection of intelligence lies in the need to overcome the determined will of the person with the secret not to allow it to be known.

29. An advanced persistent threat is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period.
    A. True
    B. False. A malware is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period.

30. One of China's well-known attack groups is Leviathan. This group has recently been escalating their attacks and targeting U.S. companies in the engineering and maritime fields that are linked to the South China Sea and some of the world's busiest trading routes.
    A. True
    B. False. One of China's well-known attack groups is Lazarus. This group has recently been escalating their attacks and targeting U.S. companies in the engineering and maritime fields that are linked to the South China Sea and some of the world's busiest trading routes.