UNIT-XV

CLOUD COMPUTING AND CYBER SECURITY

1.	Cloud Computing	1-5
2.	Cyber Security	6-12

ENGINEERS ACADEMY®
Your GATEway to Professional Excellence
IES • GATE • PSUs • JTO • IAS • NET

www. eapublications.org

NOTES

CHAPTER 1

CLOUD COMPUTING

OBJECTIVE QUESTIONS

1. Which of the following statement(s) is/are TRUE?

(i) Software as a Service delivery model is an example of a cloud computing environment that provides users with a web based email service

(ii) Platform as a Service cloud provider offers an environment for building applications that will run from the customer's environment.

(iii) Infrastructure as a Service delivery model is an example of a cloud computing environment that provides users access to virtual machines?

(a) (ii) and (iii) (b) (i) and (iii)
(c) (i),(ii) and (iii) (d) (i) and (ii)

2. A company has decided to leverage the web conferencing services provided by a cloud provider and to pay for those services as they are used. The cloud provider manages the infrastructure and any application upgrades. This is an example of what type of cloud delivery model?

(a) Software as a Service
(b) Platform as a Service
(c) Application as a Service
(d) Infrastructure as a Service

3. Which statement best describes the relationship between application, server, and client in a multitenant environment?

(a) Multiple instances of software running on multiple servers and serves one client.

(b) Single instance of software running on a server and serves one client.

(c) Single instance of software running on a server and serves multiple clients.

(d) Multiple instances of software running on a server and serves multiple client

4. Which two statements are true about the public cloud model?

(i) It meets security and auditing requirements for highly regulated industries.

(ii) Resources and infrastructure are managed and maintained by the enterprise IT operations staff.

(iii) It shifts the bulk of the costs from capital expenditures and IT infrastructure investment to an utility operating expense model.

(iv) It shifts the bulk of the costs from capital expenditures to creating a virtualized and elastic infrastructure within the enterprise data center.

(v) Resources are dynamically provisioned on a self service basis from an off site third party provider who shares resources in a multitenanted infrastructure.

(a) (iii) and (v)
(b) (i),(iv) and (v)
(c) (i),(ii) and (iv)
(d) (i),(ii) and (iii)

5. An enterprise needs highly controlled storage and access to their databases as well as managing the infrastructure for web front ends and other applications. They have a large existing IT infrastructure and they are continually expanding the capabilities. Which cloud computing model will satisfy all their current needs and enable them to reduce cost?

(a) internal cloud (b) private cloud
(c) public cloud (d) hybrid cloud

6. When will cloud computing provide the most value?

(a) A company has to process their payroll actives at the end of each pay period in batch mode.

(b) A company has several thousands of documents that need to be indexed in many months

(c) A company has purchased additional hardware in order to process their payroll activities faster at the end of each pay period.

(d) A company has several hundreds of documents that need to be indexed in a few minutes.

7. Which statement best describes the Software as a Service cloud delivery model?

(a) An application delivered to the client from the cloud which eliminates the need to install and run the application on the customer's own computers and simplifying maintenance and support.

(b) A virtual machine provisioned and provided from the cloud which allows the customer to deploy custom applications.

(c) A multitenant storage service provisioned from the cloud which allows the customer to leverage the cloud for storing software data.

(d) A solution stack or set of middleware delivered to the client from the cloud which provides services for the design, development, and testing of industry aligned applications.

8. What is grid computing?

(a) It is distributed computing where autonomous computers perform independent tasks.

(b) It is parallel computing where autonomous computers act together to perform very large tasks.

(c) It is parallel and distributed computing where computer infrastructure is offered as a service.

(d) It is interconnected computing where a computing platform is delivered to consumers.

9. A company interested in cloud computing is looking for a provider who offers a set of basic services such as virtual server provisioning and ondemand storage that can be combined into a platform for deploying and running customized applications. What type of cloud computing model fits these requirements?

(a) Platform as a Service

(b) Application as a Service

(c) Software as a Service

(d) Infrastructure as a Service

10. What is true about an application service provider?

(a) It delivers Platform as a Service.

(b) It delivers Software as a Service.

(c) It delivers Infrastructure as a Service.

(d) It delivers Communications as a Service.

11. What are two important benefits of using cloud computing?

(i) Optimizes IT investments.

(ii) Deployment of single tenant application.

(iii) Enhanced Web V2.0 interfaces for user interactions.

(iv) Lower total cost of ownership and improved asset utilization.

(v) Provides better availability than a standard computing environment.

(a) (i),(iv) and (v)

(b) (i) and (iv)

(c) (iv) and (v)

(d) (i),(ii) and (iii)

12. What is utility computing?

(a) It is an organization that maintains the computer infrastructure for a public service.

(b) It is a service model where customers pay a flat rate for usage.

(c) It is a computing model where computer resources are provided on demand.

(d) It delivers computing resources as a metered service.

13. Which statement is true about the reliability of a cloud computing solution?

(a) A cloud computing service can schedule a maintenance outage that affects the availability of the resources.

(b) A hybrid cloud strategy represents the best approach for a reliable cloud computing environment.

(c) A public cloud is less reliable than a private cloud.

(d) Cloud computing improves the reliability through the use of multiple sites.

14. Which customer scenario is best suited to maximize the benefits gained from using a virtual private cloud?

(a) An enterprise that requires minimal security over their data and has a large existing infrastructure that is capable of handling future needs.

(b) An enterprise that does not want to sacrifice security or make changes to their management practices but needs additional resources for test and development of new solutions.

(c) An enterprise whose IT infrastructure is under utilized on average and the system load is fairly consistent.

(d) A small start up business focused primarily on short term projects and has minimal security policies.

15. What is the role of virtualization in cloud computing?

(a) It improves the performance of web applications.

(b) It optimizes the utilization of computing resources.

(c) It removes operating system inefficiencies.

(d) It adds extra load to the underlying physical infrastructure and has no role in cloud computing.

16. What are the components of a cloud computing environment?

(a) client, application, session, network, data

(b) application, presentation, transport, network, data

(c) client, application, platform, infrastructure, server

(d) application, platform, infrastructure

17. Cloud service providers typically provide web based management consoles that provide users insight on the state of cloud services. What is one technology used in client side browser code that queries back end systems for data from the cloud services?

(a) PHP (b) AJAX
(c) XHTML (d) HTML

18. Which statement is true about the maintenance of a cloud computing environment?

(a) In an Infrastructure as a Service (IaaS) environment, patches are automatically installed on the clients.

(b) In a SaaS environment, customers do not need to worry about installing patches in the virtual instances.

(c) In an IaaS environment, customers do not need to worry about installing patches in the virtual instances.

(d) In a Software as a Service (SaaS) environment, patches are automatically installed on the clients.

19. What are two traits of a cloud computing architecture?

(i). single tiered

(ii). not scalable

(iii) on demand access to resources

(iv). internet/intranet accessible server

(v). client and server run in the same physical environment

(a) (i), (iii) and (v) (b) (i),(ii) and (v)
(c) (iii) and (iv) (d) (ii) and (iv)

20. Which statement is true about the security of the cloud computing environment?

(a) It is compromised because it is a shared environment.

(b) Access to critical data is better controlled in a private cloud environment.

(c) A public cloud provides the same level of security as a private cloud.

(d) Multitenant applications are not able to run in a cloud environment.

21. What is Cloud Computing replacing?

(a) Corporate data centres

(b) Expensive personal computer hardware

(c) Expensive software upgrades

(d) All of the above

22. Which of these companies is not a leader in cloud computing?

(a) Google (b) Microsoft
(c) Amazon (d) Blackboard

23. "Cloud" in cloud computing represents what?

(a) Internet (b) Wireless
(c) Hard drives (d) People

24. Which is not a major cloud computing platform?

(a) Google 101 (b) IBM Deep blue
(c) Microsoft Azure (d) Amazon EC2

25. Which of the following service provider provides the least amount of built-in security?

(a) SaaS (b) PaaS
(c) IaaS (d) None of these

26 Which of the following area of cloud computing is uniquely troublesome?

(a) Auditing

(b) Data Integrity

(c) E-Discovery for legal compliance

(d) All of the above

27. _____ serves as a PaaS vendor within Google App Engine system.

(a) Google (b) Amazon
(c) Microsoft (d) None of these

28. _____ is the most refined and restrictive service model.

(a) IaaS (b) CaaS
(c) PaaS (d) None of these

29. Which of these is not a major type of cloud computing usage?

(a) Hardware as a Service
(b) Platform as a Service
(c) Software as a Service
(d) Infrastructure as a Service

30. What is the number one concern about cloud computing?

(a) Accessibility (b) Too expensive
(c) Security concerns (d) Too many platforms

31. Which of the following type of virtualization is also characteristic of cloud computing?

(a) Storage (b) Application
(c) CPU (d) All of the Above

32. Point out the correct statement:

(a) A client can request access to a cloud service from any location

(b) A cloud has multiple application instances and directs requests to an instance based on conditions

(c) Computers can be partitioned into a set of virtual machines with each machine being assigned a workload

(d) All of the mentioned

33. _____ provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets.

(a) IaaS (b) SaaS
(c) PaaS (d) None of these

34. Point out the wrong statement :

(a) SaaS applications come in all shapes and sizes

(b) Every computer user is familiar with SaaS systems

(c) SaaS software is not customizable

(d) None of the above

❑❑❑

Answer Key

1. *Ans. (c)*
2. *Ans. (a)*
3. *Ans. (c)*
4. *Ans. (a)*
5. *Ans. (d)*
6. *Ans. (a)*
7. *Ans. (a)*
8. *Ans. (b)*
9. *Ans. (d)*
10. *Ans. (b)*
11. *Ans. (a)*
12. *Ans. (d)*
13. *Ans. (d)*
14. Ans. (b)
15. Ans. (b)
16. Ans. (c)
17. Ans. (b)
18. Ans. (b)
19. Ans. (c)
20. Ans. (b)
21. Ans. (d)
22. *Ans. (d)*
23. Ans. (a)
24. Ans. (b)
25. Ans. (c)
26. Ans. (d)
27. Ans. (a)
27. Ans. (c)
29. Ans. (a)
30. Ans. (c)
31. Ans. (d)
32. Ans. (d)
33. Ans. (a)
34. Ans. (d)

❑❑❑

CHAPTER 2

CYBER SECURITY

OBJECTIVE QUESTIONS

1. _____ is an internet-based computing solution where shared resources are provided.
   (a) Clound Computing
   (b) Networking
   (c) LAN
   (d) None of the above

2. The role of sensor in smart grid architecture of IoT is to _____.
   (a) Provide security (b) Filter data
   (c) Store data (d) Transfer data

3. Which of the following is not OWASP top 10 vulnerabilities?
   (a) Insecure Deserialization
   (b) Cross the Scripting (XSS)
   (c) Broken Authentication
   (d) Privacy Breach

4. IPv6 addresses have a size of
   (a) 64 bits (b) 128 bits
   (c) 256 bits (d) 512 bits

5. Cloud computing operates on _____ and edge computing operates on _____ generated by sensors or users respectively.
   (a) big data and real-time data
   (b) real-time data and big data
   (c) big data and dig data
   (d) real-time data and real-time data

6. Which is/are key characteristics of IoT?
   I. Safety
   II. Connectivity
   III. Heterogeneity
   (a) Only I (b) Only I and II
   (c) Only I and III (d) I, II and III

7. Block in the block chain consist of?
   I. Harse pointer
   II. Transaction data
   III. Timestamp
   (a) Only I (b) Only I and II
   (c) Only II and III (d) I, II and III

8. EC2 is an example of which service model in Cloud computing?
   (a) PaaS (b) SaaS
   (c) IaaS (d) MaaS

9. Which is the at the lowest layer in the IoT Architecture?
   (a) Smart devices
   (b) Gateway
   (c) Cloud
   (d) Service Management

10. In Edge computing the data is stored _____.
    (a) Closer to the location where it is needed.
    (b) Closer to the location where it is generated.
    (c) farthest from the location where it is generated
    (d) farthest from the location where it is needed

11. In which cyber-attack, an application accepts user inputs and allows these inputs to enter a database, shell command, or operating system, making the application susceptible.
    (a) injection
    (b) XML External Entity
    (c) Sensitive Data Exposure
    (d) Security Misconfiguration

12. Name the IoT Application for the below given statement?

"If a person coming from office gives a command to his AC to set the temperature at 24°C from his smartphone".

(a) IoT in Everyday life

(b) IoT in Health care

(c) IoT in Industrial Automation

(d) IoT in Smart Cities

13. _____ attack is a type of attack against an application that parses XML input.

(a) Injection (b) HTML

(c) XXE (d) XSS

14. Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called _____

(a) Session Spying

(b) Session Hijacking

(c) Cookie stuffing

(d) Session Fixation

15. A_____ vulnerability can allow an attacker to use manual and/or automatic methods to try to gain control over any account they want in a system - or even worse - to gain complete control over the system.

(a) Sensitive data exposure

(b) Broken Authentication

(c) XML External Entity attack

(d) Code Injection

16. What is the abbreviation of OWASP?

(a) Open Web Application Security Project

(b) Object Wide Application Security Program

(c) Object Wide Application Security Project

(d) Open Web Application Security Program

17. Which is not part of OWASP top 10 vulnerabilities?

(a) Broken Access control

(b) Broken Authentication

(c) Code Injection

(d) Infection

18. _____framework is finding and cracking vulnerabilities easily and is used by both white as well as black hat hackers.

(a) Metasploit (b) .Net

(c) Zeus (d) Ettercap

19. _____ is a code injecting method used for attacking the database of a system/website.

(a) HTML injection

(b) XML Injection

(c) Malicious code injection

(d) SQL Injection

20. An ____is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.

(a) XML External Entity attack

(b) Code Injection

(c) Broken Authentication

(d) Sensitive data exposure

21. _____is one of the most widespread vulnerabilities on the OWASP list. It consists of compromising data that should have been protected.

(a) Sensitive data exposure

(b) Code Injection

(c) XML External Entity attack

(d) Broken Authentication

22. Which is TRUE about Nmap

(i) Nmap is abbreviated as Network Mapper

(ii) Nmap is a popular tool used for discovering networks as well as in security auditing.

(iii) Nmap do not check what type of antivirus is in use

(a) (i), (ii) and (iii)

(b) (i) and (iii)

(c) (ii) and (iii)

(d) (i) and (ii)

23. What is the abbreviation of XXE & XSS vulnerabilities

(a) Cross XML Entities & XML Cross Site Scripting

(b) XML Secure Entities & XML Cross Site Scripting

(c) Cross XML Entities & XML Secure Scripting

(d) XML External Entities & Cross Site Scripting

24. Match the following

Firewalls

(i) Packet filtering firewalls

(ii) Stateful Multilayer firewalls

(iii) Application layer firewalls

Generation

P. First generation firewalls

Q. Second generation firewalls

R. Third generation firewalls

(a) (i)-Q, (ii)-P, (iii)-R
(b) (i)-R, (ii)-Q, (iii)-P
(c) (i)-Q, (ii)-R, (iii)-P
(d) (i)-P, (ii)-Q, (iii)-R

25. Find the odd man out in the context of Secure Programming?

(a) Format-string attack prevention
(b) Integer-overflow prevention
(c) Buffer-overflow prevention
(d) Denial of Service(DoS)

26. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

(a) HTML Injection
(b) Cross Site Scripting (XSS)
(c) SQL injection
(d) Cross Site Request Forgery (XSRF)

27. The full form of Malware is _____

(a) Malfunctioned Software
(b) Multipurpose Software
(c) Malicious Software
(d) Malfunctioning of Security

28. XSS is abbreviated as _____

(a) Extreme Secure Scripting

(b) Cross Site Security

(c) X Site Scripting

(d) Cross Site Scripting

29. Which of them is not a wireless attack?

(a) Eavesdropping

(b) MAC Spoofing

(c) Wireless Hijacking

(d) Phishing

30. Who deploy Malwares to a system or network?

(a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists

(b) Criminal organizations, White hat hackers, malware developers, cyber-terrorists

(c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists

(d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

31. _____ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain.

(a) Cyber-warfare (b) Cyber campaign
(c) Cyber-terrorism (d) Cyber attack

32. When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.

(a) Database crash attack

(b) DoS (Denial of Service) attack

(c) Data overflow Attack

(d) Buffer Overflow attack

33. Which is the legal form of hacking based on which jobs are provided in IT industries and firms?

(a) Cracking

(b) Non ethical Hacking

(c) Ethical hacking

(d) Hactivism

34. _____ are the combination of both white as well as black hat hackers.

(a) Grey Hat hackers

(b) Green Hat hackers

(c) Blue Hat Hackers

(d) Red Hat Hackers

35. Governments hired some highly skilled hackers. These types of hackers are termed as _____

(a) Special Hackers

(b) Government Hackers

(c) Cyber Intelligence Agents

(d) Nation / State sponsored hackers

❑❑❑

Answer Key

1. **Ans. (a)**

2. **Ans. (c)**

- In an Internet of Things (IoT) ecosystem, two things are very important : The Internet and physical devices like sensors and actuators.
- The bottom layer of the IoT system consists of sensor connectivity and network to collect information.
- The main purpose of sensors is to collect data from the surrounding environment. Sensors, or things of the IoT system, form the fron end. These are connected directly or indirectly to IoT networks after signal conversion and processing.

3. **Ans. (d)**

- WASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documenatation, tools, and technologies in the field of web application security.
- OWASP Top 10 is the list of the 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures.
- Updated every three to four years, the latest OWASP vulnerabilities list was released in 2018.

The Top 10 OWASP vulnerabilities are :

1. Injection
2. Broken Authentication
3. Sensitivive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security misconfigurations
7. Cross Side Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

4. **Ans. (b)**

- An IPv6 address has a size of **128 bits**.
- **Internet Protocol Version 6 (IPv6)** is the most recent version of the Internet Protocol (IP), the communications protocol that **provides an identification and location** system for computers on networks and routes traffic across the Internet.
- IPv6 was **developed by the Internet Engineering Task Force (IETF)** to deal with the long-anticipated problem of IPv4 address exhaustion.
- IPv6 is intended to replace IPv4.

5. **Ans. (a)**

6. **Ans. (d)**

7. **Ans. (d)**

- A blockchain is a growing list of records, called blocks, that are linked using cryptography.
- Each block contains a cryptographic hash of the previous block a time stamp, and transaction data.
- A blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a vertifiable and permanent way."

8. **Ans. (c)**

9. **Ans. (a)**

- The internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
- IoT system architecture, consists of devices, the Edge Gateway, and the Cloud.
- The lowest layer is made up of smart objects integrated with sensors.
- The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed.

- There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc.

10. Ans. (a)

11. Ans. (a)

12. Ans. (a)

- IoT is essentially a platform where embedded devices are connected to the internet, so they can collect and exchange dta with each other. It enables devices to interact, collaborte and, learn from each other's experiences just like humans do.
- Giving command to an AC from office to set temperature is IoT application in Everyday life.

13. Ans. (c)

14. Ans. (b)

Using session hijacking, which is popularly known as cookie hijacking is an exploitation method for compromising the user's session for gaining unauthorized access to user's information.

15. Ans. (b)

16. Ans. (a)

17. Ans. (d)

18. Ans. (a)

19. Ans. (d)

20. Ans. (a)

21. Ans. (a)

Sensitive data exposure is one of the most widespread vulnerabilities on the OWASP list. It consists of compromising data that should have been protected.

Examples of Sensitive Data

Some sensitive data that requires protection is:

1. Credentials
2. Credit card numbers
3. Social Security Numbers
4. Medical information
5. Personally identifiable information (PII)

Other personal information

It is vital for any organization to understand the importance of protecting users' information and privacy. All companies should comply with their local privacy laws.

Responsible sensitive data collection and handling have become more noticeable especially after the advent of the General Data Protection Regulation (GDPR). This is a new data privacy law that came into effect May 2018. It mandates how companies collect, modify, process, store, and delete personal data originating in the European Union for both residents and visitors.

There are two types of data:

1. Stored data - data at rest
2. Transmitted data - data that is transmitted internally between servers, or to web browsers

22. Ans. (a)

(i) TRUE: Nmap is abbreviated as Network Mapper

(ii) TRUE: Network Mapper (Nmap) is a popular open-source tool used for discovering network as well as security auditing. It can be used for either a single host network or large networks.

(iii) TRUE: Network Mapper (Nmap) is a popular open-source tool used for discovering network as well as security auditing. It usually checks for different services used by the host, what operating system it is running and the type of firewall it is using.

23. Ans. (d)

- An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.

  Most XML parsers are vulnerable to XXE attacks by default. That is why the responsibility of ensuring the application does not have this vulnerability lays mainly on the developer.

- Cross Site Scripting (XSS) is a widespread vulnerability that affects many web applications. XSS attacks consist of injecting malicious client-side scripts into a website and using the website as a propagation method.

  The risks behind XSS is that it allows an attacker to inject content into a website and modify how it is displayed, forcing a victim's browser to execute the code provided by the attacker while loading the page.

24. Ans. (d)

25. Ans. (d)

- Buffer overflows, a common software security vulnerability, happen when a process tries to store data beyond a fixed-length buffer. For example, if there are 8 slots to store items in, there will be a problem if there is an attempt to store 9 items. In computer memory the overflowed data may overwrite data in the next location which can result in a security vulnerability (stack smashing) or program termination (segmentation fault).
- A Format String Attack is when a malicious user supplies specific inputs that will eventually be entered as an argument to a function that performs formatting, such as printf(). The attack involves the adversary reading from or writing to the stack.
- Integer overflow occurs when an arithmetic operation results in an integer too large to be represented within the available space. A program which does not properly check for integer overflow introduces potential software bugs and exploits.

26. Ans. (b)

27. Ans. (c)

Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

28. Ans. (d)

Cross Site Scripting is another popular web application attack type that can hamper the reputation of any site.

29. Ans. (d)

Wireless attacks are malicious attacks done in wireless systems, networks or devices. Attacks on Wi-Fi network is one common example that general people know. Other such sub-types of wireless attacks are wireless authentication attack, Encryption cracking etc

30. Ans. (a)

Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware devel

31. Ans. (c)

Cyber- terrorism is the term used to describe internet terrorism, where individuals and groups are anonymously misusing ethnicities, religions as well as threaten any technology user, which may lead to even loss of life.

32. Ans. (d)

The Buffer overflow attack takes place when an excessive amount of data occurs in the buffer, which it cannot handle and lead to data being overflow into its adjoined storage. This attack can cause a system or application crash and can lead to malicious entry-point.

33. Ans. (c)

Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

34. Ans. (a)

Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other's systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

35. Ans. (d)

Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

❑❑❑