ITC61Chapter10

Richard Neil P. Martinez

1. Futuristic technology refers to highly advanced technologies with the potential to revolutionize how individuals go about their daily routines, impacting diverse areas like businesses, social interactions, governance, research, and various industries.

2. Some of the top futuristic technologies mentioned in the provided context are:

1. 3D Printing Technology
2. 6G Technology
3. Autonomous Robots
4. Artificial Neurons
5. Artificial General Intelligence (AGI)
6. Mind Uploading
7. Driverless Vehicles
8. Infrastructure Hacking
9. Regenerative Medicine
10. Digital Twin (DT) Technology
11. Programmable Living Robots
12. Human Augmentation
13. Intelligent Process Automation (IPA)
14. Space Elevator
15. Rotating Skyhook
16. Light Sail

These technologies are expected to shape the future in various industries and domains.

3. The concept and process of 3D printing was introduced by Murray Leinster in 1945. The history of 3D printing dates back to the 1940s when the idea of three-dimensional printing first emerged.

4. The utilization of 3D printing spans a wide array of industries, demonstrating its versatility and growth. Key sectors benefiting from 3D printing include manufacturing, fashion, firearm production, healthcare, transportation, aviation, cultural preservation, and education.

5. 6G technology differs from other technologies in several key ways. 6G offers more throughput and much lesser latency compared to 5G networks, making it faster and more efficient. It is also supporting more advanced ICT technologies such as virtual reality, augmented reality, Internet of Things, mobile edge computing, quantum computing, and others.

6. The need for 6G technology arises from the increasing demand for higher efficiency, reduced costs, improved processes, and enhanced service quality across industries. With the exponential growth in connected devices and data bandwidth requirements, current technologies are not efficient enough to meet future demands.

7. A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It typically includes redundant or backup power supplies, redundant data communications connections, environmental controls, and security devices.

8. An autonomous robot is an intelligent machine that can perform tasks without any intervention from a human being. These robots can act based on the intelligence they possess through computer-vision training data sets.

9. Autonomous Mobile Robots (AMRs) are intelligent machines that can perform tasks without the need for human intervention. They are equipped with the ability to navigate and operate independently based on the intelligence they possess through computer-vision training datasets.

10. Artificial neurons are useful in the sense that they mimic the functioning of biological neurons in the human brain. They receive input data from multiple sources, process it through logical algorithms, and generate an output based on the importance of the input data.

11. AGI stands for Artificial General Intelligence, which is a mid-level artificial intelligence that is defined as part of human intelligence. It can handle abstract thinking, maintain background knowledge, use common sense capability, transfer learning, predict effects and causes of an event, and more.

12. Digital Twin technology helps in saving costs by reducing prototyping expenses and minimizing operational failures of products and processes significantly. It allows for better decision-making based on processed and valuable information that flows from the virtual environment to the physical environment.

ITC61Chapter11

1. Modern technologies impact cybersecurity in many ways. The increased use of a huge number of devices in diverse IoT environments, the mismanagement of user accounts and passwords, outdated software and devices, and the continual emergence of innovative techniques all contribute to data exposure and cybersecurity risks.

2. Advanced technologies are significantly impacting cybersecurity by empowering hackers and malicious users. These technologies, such as artificial intelligence, machine learning, data analytics, big data, natural language processing, and others, provide sophisticated tools for cyber attackers to exploit vulnerabilities in emerging technologies.

3. The risks associated with extensive data exposure include the use of a huge number of devices in highly diverse IoT environments where diverse firmware and software run, increased number of user accounts leading to data exposure, mismanagement in password creation and storage by clients.

4. Yes, there are strategies for controlling cyber breaches. Some common strategies include continual monitoring and updating of software and hardware tools, training staff and users for maintaining security, using advanced technologies like blockchain and artificial intelligence in cybersecurity systems, and implementing communication encryption for data storage and transportation.

5. The shortage of cybersecurity professionals is primarily due to the rapid growth in the demand for skilled and qualified cybersecurity experts and specialists. This demand is continuously increasing, while the availability of cybersecurity professionals is depleting.

6. Cyber-attacks have a significant impact on businesses. They can lead to financial losses, damage business reputation, disrupt operations, compromise sensitive data, and result in legal consequences.

7. The main reasons for data exposure pertaining to modern and innovative technologies including use of a huge number of devices in highly diverse environments of IoT where a large number of devices run diverse firmware and software. It is also increased number of user accounts with those huge numbers of devices and related services are also prone to data exposure.

8. Risk refers to the potential for loss, harm, or negative outcomes resulting from various factors or events.

9. Cybersecurity can affect national security in many ways. Some of the impacts include direct cyber attacks on security institutions, agencies, and their assets, as well as disturbances to the entire ecosystem of a nation leading to chaos and internal disturbances.

10. A Zero Trust policy is an approach to cybersecurity that assumes that threats could be both inside and outside of a network.