Bayot, July

ITC61 Chapter 10.

1. Futuristic technology can be defined as advancements or innovations that have the potential to significantly impact various aspects of human life across different domains such as businesses, social activities, governments, research and development, and a range of industries. These technologies often emerge from fields such as information and computer technology (ICT), manufacturing, aeronautics, biotechnology, nanotechnology, robotics, and others. They are characterized by their ability to push the boundaries of what is currently possible, leading to new processes, products, and industries, and ultimately reshaping the way humans live and interact with technology.

2. The top futuristic technologies:

- 3D Printing Technology
- 6G Technology
- Autonomous Robots
- Artificial Neurons
- Artificial General Intelligence (AGI)
- Mind Uploading
- Driverless Vehicles
- Infrastructure Hacking
- Regenerative Medicine
- Digital Twin (DT) Technology
- Programmable Living Robots
- Human Augmentation
- Intelligent Process Automation (IPA)
- Space Elevator
- Rotating Skyhook
- Light Sail

These technologies are poised to revolutionize various industries and processes, ushering in a new era of innovation and transformation in human activities and lifestyles.

3. 3D printing began with the conceptualization of the idea in the 1940s by Murray Leinster. Subsequently, in the 1950s, Raymond Jones published the concept in a science fiction magazine. The actual development and patents for various 3D printing techniques started in the 1970s and 1980s, with notable contributions from Johannes Gottwald, Hideo Kodama, Bill Masters, Alain Le Mehaute, and others. The technology evolved over the decades, with advancements in processes such as powder bed fusion, selective laser melting, and fused deposition modeling (FDM), leading to its widespread adoption in various industries.

4. The applications of 3D printing span across different industries and sectors. Some of the key applications include manufacturing (for prototyping and end-use parts), fashion (customized clothing and accessories), healthcare (prosthetics, implants, surgical guides), transportation (aircraft components, automotive parts), firearms (customized firearm production), education (STEM education aids), and even food production (3D printed food items). Additionally, 3D printing has been used for creating metal bridges, replicating cultural heritage artifacts, and manufacturing Personal Protective Equipment (PPE) during the COVID-19 pandemic.

5. 6G technology differs from other technologies, particularly its predecessor 5G, in several key aspects:

- 6G offers even higher data throughput and much lower latency compared to 5G networks.
- It supports more advanced technologies such as virtual reality, augmented reality, Internet of Things (IoT), and mobile edge computing.
- 6G utilizes millimeter waves in a broader spectrum range, including terahertz frequencies, to achieve higher speeds and capacity.
- It aims to fully support AI-driven applications in real-time environments, such as autonomous vehicles, powered by artificial intelligence.

6. The need for 6G technology arises from the increasing demand for higher data bandwidth, lower latency, and support for emerging technologies and services. Existing

technologies, including 5G, may not be sufficient to meet the future demands of industries such as IoT, edge computing, high-performance computing, and virtualization. Therefore, 6G technology is essential for enabling advanced services, enhancing connectivity, and driving innovation across various sectors.

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 (e.g., air conditioning, fire suppression), and security devices. Data centers are used to store, manage, and distribute large amounts of data and are essential for the operation of various online services, websites, and cloud computing platforms.

8. An autonomous robot is an intelligent machine capable of performing tasks without human intervention. It relies on its own intelligence, usually acquired through computer-vision training datasets, to execute tasks autonomously.

9. Autonomous mobile robots (AMRs) are self-operating and self-maintaining machines designed to perform tasks without human assistance. They are capable of navigating through various environments, overcoming obstacles, and executing designated tasks efficiently. AMRs find applications in industries such as logistics, ecommerce, manufacturing, warehousing, healthcare, and research and development (R&D).

10. Artificial neurons are useful because they mimic the functionality of biological neurons in human brains, allowing them to process data, make decisions, and pass on results to other neurons or layers of a neural network. They play a key role in artificial intelligence and machine learning applications.

11. AGI stands for Artificial General Intelligence, which aims to develop machine intelligence matching human-level decision-making capabilities. ASI, or Artificial Super Intelligence, represents the most advanced form of AI, surpassing even the most brilliant human minds in various cognitive tasks.

12. Digital Twin (DT) technology is important because it creates virtual replicas of physical objects, processes, or systems, allowing for real-time monitoring, analysis, and optimization. This technology enhances efficiency, reduces costs, and enables predictive

maintenance in various industries such as manufacturing, healthcare, and smart cities development.

ITC61 Chapter 11.

1. Modern technologies expand the threat surface in cybersecurity by introducing new vulnerabilities and providing hackers with more opportunities to exploit security loopholes.
2. Advanced technologies increase cybersecurity challenges by introducing complexities in operations and maintenance, facilitating the use of sophisticated hacking tools, and creating compatibility issues with existing systems.
3. Extensive data exposure poses risks such as unauthorized access, data breaches, identity theft, and manipulation of sensitive information, leading to financial losses, reputation damage, and privacy violations.
4. Yes, strategies for controlling cyber breaches include continual monitoring and updating of software and hardware, employee training, encryption for data storage and transmission, use of secure technologies like blockchain and AI, behavior analytics, and implementing a zero-trust policy
5. The shortage of cybersecurity professionals is due to the increasing demand for skilled experts in the field, lack of adequate training programs, rapid advancements in technology, and the complexity of cyber threats.
6. Cyber-attacks can have significant impacts on businesses, including financial losses, damage to reputation, disruption of operations, loss of sensitive data, and legal consequences.
7. Main reasons for data exposure include the use of outdated software and devices, mismanagement of passwords, increasing number of IoT devices with diverse firmware, and continual emergence of innovative hacking techniques.
8. Risk refers to the possibility of loss, damage, or harm resulting from exposure to various threats or uncertainties.

9. Cybersecurity can affect national security by safeguarding critical infrastructure, protecting sensitive government information, defending against cyber espionage and sabotage, and preventing disruption to essential services.
10. Zero trust policy is an approach to cybersecurity that requires strict verification of every user and device attempting to access a network, regardless of whether they are inside or outside the network perimeter.