Graduate Certificate in Anthropology of the Internet and Digital Cultures

Cybersecurity and Privacy

Cybersecurity
Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks. These attacks can come in various forms, such as malware, phishing, ransomware, and denial-of-service attacks. Cybersecurity measures are put in place to prevent unauthorized access to sensitive information and to ensure the confidentiality, integrity, and availability of data.

Privacy
Privacy is the right of individuals to control how their personal information is collected, used, and shared. In the context of digital cultures, privacy concerns arise from the vast amount of data that is collected online through social media, search engines, and other digital platforms. Individuals may be concerned about their privacy being compromised through data breaches, surveillance, or targeted advertising.

Encryption
Encryption is the process of encoding information in such a way that only authorized parties can access it. This is done by using cryptographic algorithms to convert plain text into ciphertext, which can only be decrypted with the appropriate key. Encryption is essential for protecting sensitive data in transit and at rest.

Firewall
A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls are commonly used to protect networks from unauthorized access and cyberattacks.

Vulnerability
A vulnerability is a weakness in a system or network that can be exploited by attackers to compromise the security of the system. Vulnerabilities can exist in software, hardware, or human processes, and they can be exploited through various means, such as malware, phishing, or social engineering.

Phishing
Phishing is a type of cyberattack in which attackers use fraudulent emails, messages, or websites to trick individuals into providing sensitive information, such as login credentials or financial details. Phishing attacks often impersonate legitimate organizations to deceive recipients into disclosing confidential information.

Ransomware
Ransomware is a type of malware that encrypts a victim's files or locks their computer system, demanding a ransom payment in exchange for restoring access to the data. Ransomware attacks can have devastating consequences for individuals and organizations, causing data loss and financial damages.

Multi-factor authentication
Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more forms of verification before granting access to a system or application. This typically involves something the user knows (such as a password), something they have (such as a smartphone), or something they are (such as a fingerprint).

Zero-day exploit
A zero-day exploit is a cyberattack that takes advantage of a previously unknown vulnerability in software or hardware. Zero-day exploits are particularly dangerous because they give attackers the element of surprise, as security patches or updates may not be available to defend against the exploit.

Social engineering
Social engineering is a technique used by cybercriminals to manipulate individuals into divulging confidential information or performing actions that compromise security. This can involve impersonating trusted entities, such as tech support or coworkers, to gain access to sensitive data.

Penetration testing
Penetration testing, also known as ethical hacking, is the practice of simulating cyberattacks on a system or network to identify vulnerabilities that could be exploited by malicious actors. Penetration testers use ethical means to assess the security posture of an organization and recommend remediation measures.

Incident response
Incident response is the process of reacting to and managing cybersecurity incidents, such as data breaches, malware infections, or denial-of-service attacks. An effective incident response plan includes procedures for detecting, analyzing, containing, and recovering from security breaches.

End-to-end encryption
End-to-end encryption is a method of securing communication between two parties by encrypting the data in such a way that only the sender and the recipient can decrypt it. End-to-end encryption ensures that messages or data cannot be intercepted or read by unauthorized parties, even service providers.

Access control
Access control is the practice of restricting access to systems, networks, or data to authorized users only. Access control mechanisms include user authentication, authorization, and audit trails to ensure that users have the appropriate permissions to access resources.

Security awareness training
Security awareness training is an educational program designed to teach employees about cybersecurity threats and best practices for protecting sensitive information. Training topics may include phishing awareness, password security, and social engineering tactics to help employees recognize and respond to potential security risks.

Data breach
A data breach occurs when unauthorized individuals gain access to sensitive or confidential data, either through cyberattacks, insider threats, or human error. Data breaches can have serious consequences for

individuals and organizations, leading to financial losses, reputational damage, and legal penalties.

Compliance
Compliance refers to the adherence to laws, regulations, and industry standards related to cybersecurity and privacy. Organizations are required to comply with data protection laws, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), to protect the privacy of individuals' data.

Security policy
A security policy is a set of rules and procedures that outline an organization's approach to cybersecurity and privacy management. Security policies define the roles and responsibilities of employees, the acceptable use of technology resources, and the measures to protect sensitive information from unauthorized access.

Virtual private network (VPN)
A virtual private network (VPN) is a technology that creates a secure, encrypted connection over a public network, such as the internet. VPNs are commonly used to protect online privacy, bypass geo-restrictions, and secure data transmissions between remote users and corporate networks.

Internet of Things (IoT)
The Internet of Things (IoT) refers to the network of interconnected devices, sensors, and appliances that communicate and exchange data over the internet. IoT devices can include smart thermostats, wearables, and home security systems, which may pose security risks if not properly secured.

Blockchain
Blockchain is a decentralized, distributed ledger technology that securely records transactions across multiple computers in a tamper-proof manner. Blockchain is often associated with cryptocurrencies like Bitcoin, but it has broader applications in supply chain management, voting systems, and identity verification.

Cyber hygiene
Cyber hygiene refers to the best practices and habits that individuals and organizations should follow to maintain good cybersecurity hygiene. This includes keeping software up to date, using strong passwords, avoiding suspicious links, and regularly backing up data to prevent cyber threats.

Dark web
The dark web is a part of the internet that is not indexed by traditional search engines and requires special software, such as Tor, to access. The dark web is often associated with illegal activities, such as drug trafficking, cybercrime, and the sale of stolen data or malware.

Digital footprint
A digital footprint is the trail of data left behind by individuals when they use online services, such as social media, search engines, or e-commerce platforms. Digital footprints can include personal information, browsing history, and interactions with online content, which may be used for targeted advertising or profiling.

Data protection impact assessment (DPIA)
A data protection impact assessment (DPIA) is a process used to identify and mitigate privacy risks associated with a particular data processing activity. DPIAs help organizations assess the impact of data processing on individuals' privacy rights and implement measures to comply with data protection regulations.

Biometric authentication
Biometric authentication uses unique physiological or behavioral characteristics, such as fingerprints, facial recognition, or iris scans, to verify the identity of individuals accessing a system or device. Biometric authentication offers a more secure and convenient alternative to traditional password-based authentication methods.

Supply chain security
Supply chain security involves protecting the flow of goods, services, and information from suppliers to consumers against cybersecurity threats. Supply chain security measures aim to ensure the integrity and confidentiality of data exchanged between partners and prevent supply chain disruptions caused by cyberattacks.

Cyber insurance
Cyber insurance is a type of insurance policy that helps organizations mitigate financial losses resulting from cyber incidents, such as data breaches, ransomware attacks, or business interruptions. Cyber insurance policies may cover costs related to data recovery, legal fees, and regulatory fines.

Artificial intelligence (AI)
Artificial intelligence (AI) refers to the simulation of human intelligence processes by machines, such as learning, reasoning, and problem-solving. AI technologies are increasingly used in cybersecurity to detect and respond to cyber threats, automate security operations, and improve threat intelligence.

Machine learning
Machine learning is a subset of artificial intelligence that enables computers to learn from data and make predictions or decisions without being explicitly programmed. Machine learning algorithms are used in cybersecurity to analyze patterns, detect anomalies, and identify potential security threats in real-time.

Red team vs. blue team
In cybersecurity, the red team and blue team are two groups of professionals who simulate cyberattacks and defense strategies to test and improve an organization's security posture. The red team acts as the adversary, attempting to breach security controls, while the blue team defends against the attacks and evaluates the effectiveness of security measures.

Internet censorship
Internet censorship refers to the control or suppression of online content, communication, or access by governments, organizations, or internet service providers. Censorship measures may restrict freedom of speech, limit access to information, or block websites deemed to be harmful or illegal in a specific jurisdiction.

Deepfake
Deepfake is a type of synthetic media generated by artificial intelligence that combines and superimposes existing images and videos onto source images or videos, often creating realistic but fake content. Deepfake technology can be used to manipulate audiovisual content for malicious purposes, such as spreading misinformation or impersonating individuals.

Cyberbullying
Cyberbullying refers to the use of digital communication tools, such as social media, messaging apps, or online forums, to harass, intimidate, or threaten individuals. Cyberbullying can have serious psychological and emotional effects on victims and may lead to social isolation, depression, or even suicide in extreme cases.

Digital rights management (DRM)
Digital rights management (DRM) is a technology used to control access to digital content and protect intellectual property rights, such as music, movies, or software. DRM systems enforce restrictions on how digital content can be used, copied, or distributed to prevent unauthorized sharing or piracy.

Internet of Bodies (IoB)
The Internet of Bodies (IoB) refers to the network of interconnected wearable devices, implantable sensors, and medical devices that collect and transmit biometric data about the human body. IoB technologies raise concerns about privacy, security, and data ownership, as personal health information becomes increasingly digitized and shared.

Zero trust security model
The zero trust security model is an approach to cybersecurity that assumes no trust in users, devices, or networks, both inside and outside an organization's perimeter. Zero trust principles include verifying identities, enforcing least privilege access, and continuously monitoring and analyzing network activity to detect and respond to security threats.

Homomorphic encryption
Homomorphic encryption is a type of encryption that allows for computations to be performed on encrypted data without decrypting it first. Homomorphic encryption enables secure data processing in the cloud or other third-party environments while preserving the confidentiality of sensitive information.

Cyber resilience
Cyber resilience is the ability of an organization to prepare for, respond to, and recover from cyber incidents while maintaining business operations and minimizing the impact of disruptions. Cyber resilience strategies include risk assessments, incident response planning, and business continuity measures to ensure continuity in the face of cyber threats.

Internet of Behaviors (IoB)
The Internet of Behaviors (IoB) is a concept that combines data from the Internet of Things (IoT) with behavioral analytics to track, analyze, and influence human behaviors. IoB technologies raise concerns about privacy, surveillance, and ethical implications, as personal behaviors are monitored and used to shape

consumer choices.

Privacy by design
Privacy by design is a framework that promotes the integration of privacy and data protection principles into the design and development of systems, products, and services from the outset. Privacy by design aims to proactively address privacy risks, enhance user trust, and ensure compliance with data protection regulations.

Threat intelligence
Threat intelligence is information about potential or current cyber threats, including indicators of compromise, vulnerabilities, and tactics used by threat actors. Threat intelligence is used by cybersecurity professionals to proactively defend against cyber threats, detect security incidents, and respond to emerging risks.

Internet of Medical Things (IoMT)
The Internet of Medical Things (IoMT) refers to connected medical devices, wearables, and healthcare systems that collect and transmit patient data over the internet. IoMT technologies offer opportunities to improve healthcare delivery, but they also raise concerns about data security, patient privacy, and regulatory compliance.

Cybersecurity governance
Cybersecurity governance refers to the framework of policies, processes, and controls that guide an organization's approach to managing cybersecurity risks. Cybersecurity governance involves establishing roles and responsibilities, defining risk tolerance, and aligning security initiatives with business objectives to protect critical assets.

Dark data
Dark data refers to the vast amount of unstructured, unused, or hidden data that organizations collect but do not analyze or leverage for insights. Dark data poses privacy and security risks, as it may contain sensitive information that could be exposed in a data breach or misused for malicious purposes.

Security information and event management (SIEM)
Security information and event management (SIEM) is a technology solution that provides real-time monitoring, analysis, and correlation of security events and logs across an organization's network. SIEM systems help security teams detect and respond to security incidents, investigate threats, and comply with regulatory requirements.

Internet of Voice (IoV)
The Internet of Voice (IoV) refers to the interconnected ecosystem of voice-activated devices, virtual assistants, and smart speakers that enable users to interact with technology using voice commands. IoV technologies raise privacy concerns about voice data collection, storage, and third-party access to audio recordings.

Quantum cryptography
Quantum cryptography is a branch of quantum physics that uses quantum mechanics principles to secure

communication channels against eavesdropping and interception. Quantum cryptography leverages quantum properties, such as superposition and entanglement, to generate secure encryption keys that cannot be intercepted or copied by adversaries.

Cyber-physical systems (CPS)
Cyber-physical systems (CPS) are interconnected networks of physical devices, sensors, and computing systems that monitor and control physical processes in real-time. CPS applications include smart grids, autonomous vehicles, and industrial control systems, which require robust cybersecurity measures to protect against cyber threats.

Privacy-enhancing technologies (PETs)
Privacy-enhancing technologies (PETs) are tools and techniques designed to protect individuals' privacy and data security in digital environments. PETs include encryption, anonymization, data minimization, and access control mechanisms that help mitigate privacy risks and empower individuals to control their personal information.

Cyber sovereignty
Cyber sovereignty is the concept that states have the right to govern and control the internet within their borders, including regulating online content, data flows, and cyberspace activities. Cyber sovereignty raises debates about internet freedom, censorship, and the balance between national security and individual rights in the digital age.

Decentralized identity
Decentralized identity is a digital identity model that empowers individuals to own, manage, and control their personal data without relying on centralized authorities or intermediaries. Decentralized identity solutions leverage blockchain, distributed ledger technology, and self-sovereign identity principles to enhance privacy and security in digital interactions.

Threat hunting
Threat hunting is a proactive cybersecurity practice that involves actively searching for signs of potential cyber threats or security incidents within an organization's network. Threat hunters use advanced analytics, threat intelligence, and behavioral analysis techniques to detect and respond to hidden threats before they escalate.

Security token
A security token is a digital asset that represents ownership or rights to a specific security or financial instrument, such as shares, bonds, or commodities. Security tokens are issued and traded on blockchain platforms, offering greater transparency, liquidity, and compliance with securities regulations compared to traditional securities.

Internet of Everything (IoE)
The Internet of Everything (IoE) refers to the interconnected network of people, devices, data, and processes that enable intelligent communication and collaboration in the digital world. IoE technologies integrate the Internet of Things (IoT), Internet of Services (IoS), and Internet of People (IoP) to create a hyper-connected

ecosystem.

Security operations center (SOC)
A security operations center (SOC) is a centralized facility that houses cybersecurity professionals, tools, and technologies to monitor, detect, analyze, and respond to security incidents in real-time. SOCs play a critical role in maintaining the security posture of organizations and ensuring rapid incident response to cyber threats.

Unified threat management (UTM)
Unified threat management (UTM) is a comprehensive security solution that combines multiple security features, such as firewall, intrusion detection, antivirus, and virtual private network (VPN), into a single platform. UTM appliances offer simplified security management, enhanced threat detection, and integrated protection against various cyber threats.

Vulnerability management
Vulnerability management is the practice of identifying, prioritizing, and mitigating security vulnerabilities in systems, applications, and networks to reduce the risk of cyberattacks. Vulnerability management processes include vulnerability scanning, patch management, and remediation strategies to address weaknesses and enhance cybersecurity resilience.

Security token offering (STO)
A security token offering (STO) is a fundraising method that involves issuing digital tokens representing securities, such as equity or debt, on blockchain platforms to raise capital from investors. STOs comply with securities regulations and offer token holders ownership rights, dividends, or other financial benefits tied to the underlying assets.

Zero-day vulnerability
A zero-day vulnerability is a security flaw in software, hardware, or firmware that is known to the public before the vendor releases a patch or fix to address the issue. Zero-day vulnerabilities pose significant risks for organizations, as attackers can exploit them to launch targeted cyberattacks and bypass security controls.

Privacy shield
Privacy shield is a framework established by the European Union (EU) and the United States (US) to facilitate transatlantic data transfers while ensuring data protection and privacy rights for European citizens. The EU-U.S. Privacy Shield framework sets standards for data security, transparency, and redress mechanisms for companies handling personal data.

Advanced persistent threat (APT)
An advanced persistent threat (APT) is a sophisticated, long-term cyberattack orchestrated by highly skilled threat actors, such as nation-state actors or organized crime groups, to infiltrate and compromise targeted organizations. APTs involve stealthy tactics, persistent monitoring, and customized malware to evade detection and maintain access to sensitive data.

Security architecture

Security architecture refers to the design and structure of an organization's security controls, technologies