IMPORTANT!

CSA 7113T CYBER SECURITY

Complete BCA Notes (Units 1 - 5)

Notes created by
Kamal Kishor
(HandNotes)

UNIT 1: CYBERSPACE & ARCHITECTURE

1. Cyberspace Definition:

Virtual environment created by interconnected computer systems, networks, servers, internet infrastructure, and digital communication technologies where information is created, stored, exchanged, and accessed.

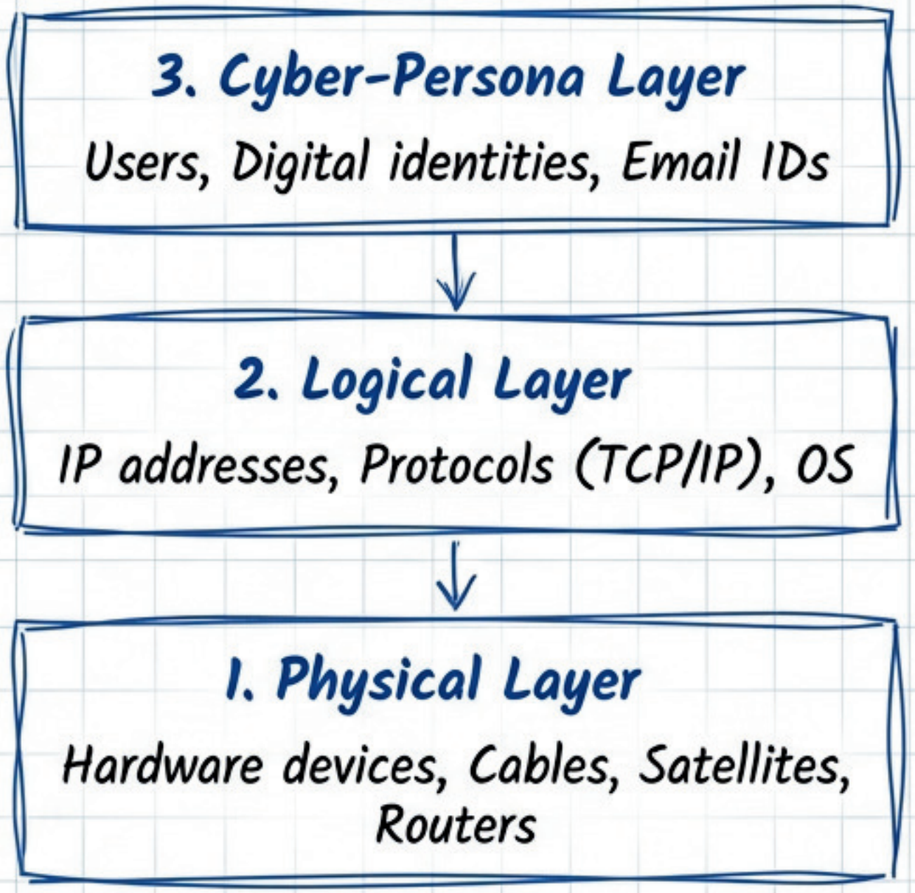
Characteristics:

- Virtual and borderless
- Depends on internet infrastructure
- Enables communication/commerce
- Vulnerable to cyber threats

Components:

- Hardware
- Software
- Networks
- Data
- Users

2. Architecture of Cyberspace (3 Layers)



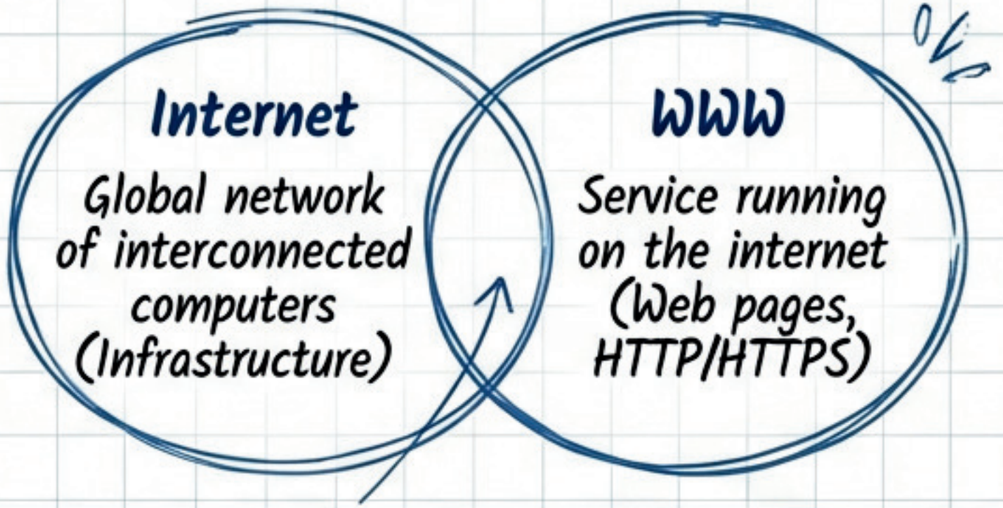
⚠ Note: Logical vulnerabilities (bugs) happen in Layer 2.

COMMUNICATION TECH & INTERNET INFRASTRUCTURE

1. Technology Stack

- **Communication:** Email, VoIP, Video Conferencing
- **Web Tech:** HTML, CSS, JavaScript
- **Client-Server Model:** Browser requests data → Server responds

2. Internet vs. WWW



3. Advent & Governance

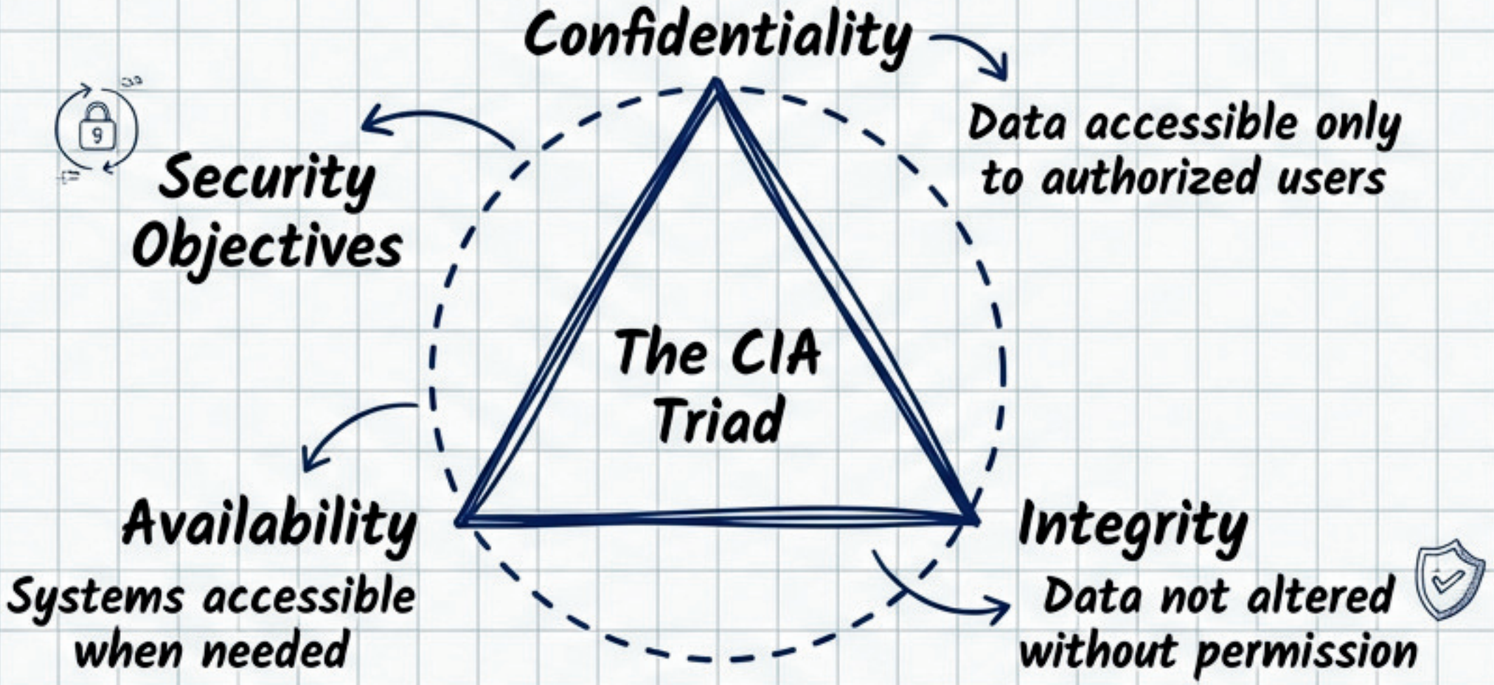
ARPANET (1960s) → TCP/IP → Commercial Internet (1990s) → Mobile/Cloud Era

- **Infrastructure Components:** ISPs, Data Centers, DNS Servers, Submarine Cables, IXPs
- **Governance:** Domain management, IP allocation, Cyber laws

Internet Society = Open Development

Concept of Cyber Security

Practice of protecting systems, networks, programs, and data from digital attacks.



Issues & Challenges

- Data breaches & Identity theft
- Cyber terrorism
- Lack of awareness & Insider threats
- Rapid technological changes

Regulation: Cyberspace is governed by Cyber Laws & IT Act.

UNIT 2: CLASSIFICATION OF CYBER CRIMES

Definition: Illegal activity performed using computers, networks, or the internet.

1. Against Individuals

- Identity theft
- Cyber stalking
- Online harassment
- Email spoofing

2. Against Property

- Data theft
- Intellectual property theft
- Malware attacks
- Software piracy

3. Against Organizations

- Hacking
- DDoS attacks
- Ransomware
- Corporate espionage

4. Against Government

- Cyber terrorism
- Website defacement
- Espionage (Threatens national security)

ATTACK VECTORS & COMMON CRIMES

1. Social Engineering (Psychological Manipulation)

- ↳ **Phishing:** Fraudulent emails/links.
- ↳ **Vishing:** Voice-based phone fraud.
- ↳ **Smishing:** SMS malicious links.
- ↳ **Pretexting:** Creating fake scenarios.

2. Malware Types

- ↳ **Virus:** Attaches to files.
- ↳ **Virus:** Attaches to files.
- ↳ **Worm:** Spreads automatically.
- ↳ **Trojan:** Disguised as safe software.
- ↳ **Spyware:** Monitors user activity.
- ↳ **Ransomware:** Encrypts data → Demands money.

3. Advanced Attacks

- ↳ **Zero Day:** Exploits unknown vulnerability (no patch).
- ↳ **Zero Click:** No user interaction required.

4. Crimes against Women/Children

- ↳ Cyber bullying, Revenge porn, Grooming.

The Legal Shield: IT Act 2000

Important Sections

- Section 43: Unauthorized access / Data damage.
- Section 66: Computer-related offences (Hacking, Identity theft).
- Section 67: Publishing obscene content.

Organizations Dealing with Cyber Crime (India):

- CERT-In: Computer Emergency Response Team (Handles incidents).
- MeitY: Ministry of Electronics & IT.
- Cyber Crime Cells: Police investigation units.
- National Cyber Coordination Centre.

Unit 3: Social Media Landscape

Definition: Online platforms for connection, communication, and content sharing.

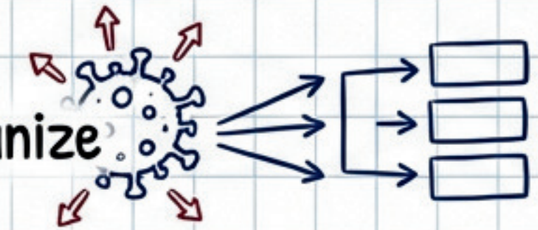
Types of Social Media

- Social Networking: Facebook, LinkedIn (Connections).
- Media Sharing: Instagram, YouTube (Photos/Video).
- Microblogging: Twitter/X (Short messages).
- Forums: Reddit, Quora (Discussions).

Social Media Monitoring

- Tracking activities for:
  - Brand reputation
  - Security threats
  - Content moderation

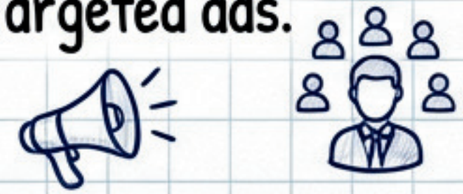
Key Terms



- Hashtags (#): Categorize and organize content.
- Viral Content: Spreads rapidly (Risk of misinformation ⚠).

Marketing

- Influencer marketing,
- Targeted ads.



SOCIAL MEDIA: RISKS & PRIVACY

Privacy Risks

Patrick Hand

- Data scraping & Info leakage.
- Location tracking.
- Identity theft from oversharing.
- Security Issues: Phishing links, Fake profiles, Malware in videos.

Challenges & Marketing Pitfalls

Patrick Hand

- Marketing: Fake influencers, Click fraud, Phishing ads.
- Addiction: Excessive use.
- Cyber Bullying: Harassment.
- Fake News: Misinformation causing panic.

CAUTION

Governance & Safe Practices

Flagging & Laws

Reporting: Use platform tools to flag abuse.

Laws: **IT Act** & **IPC** apply to **hate speech, threats**, and **obscene material.**

Best Practices Checklist

- [x] Strong passwords & 2FA.
- [x] Review privacy settings.
- [x] Avoid clicking unknown links.
- [x] Limit personal info sharing.

Case Studies

Data Breach: Facebook (Millions of profiles exposed).

Fake News: Incidents causing public **unrest.**

Data Its
dnen boad
ocovers.

Account Hacking: Instagram/Twitter takeovers.

Unit 4: E-Commerce Security

Definition: Buying/selling goods & services via electronic networks.

Buyer → Website → Payment Gateway → Seller → Logistics

Elements of Security

- ✓ Authentication: Users are genuine.
- ✓ Integrity: Data not altered.
- ✓ Confidentiality: Card numbers secret.
- ✓ Non-Repudiation: Cannot deny transaction.

Threats

✗ Phishing, Fake websites, Payment fraud.

Best Practices

SSL/TLS encryption, Regular audits, Fraud detection.

DIGITAL PAYMENT MODES

Stakeholders: Customers, Banks, Providers, Merchants

Modes of Payment

1. **Banking Cards (Debit/Credit):** Use CVV & OTP. Vulnerable to skimming.

2. **UPI (Unified Payments Interface):** Instant bank-to-bank via mobile. Uses Virtual Payment Address (VPA). High security.

3. **E-Wallets:** Store digital money (e.g., Paytm).

4. **USSD:** Banking without internet (feature phones).

5. **AEPS:** Aadhaar Enabled Payment System (Biometric auth).

PAYMENT FRAUDS & PREVENTION

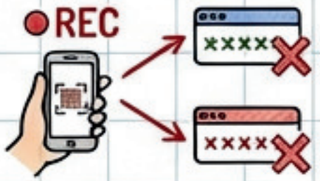
Common Frauds

OTP Fraud: Sharing One Time Password.

QR Scams: Scanning to 'receive' money (You scan = You pay!).

Fake UPI Apps: Stealing credentials.

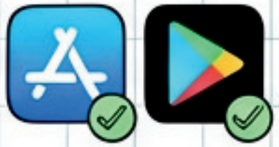
Screen-sharing scams.



Prevention Measures

NEVER share OTP or PIN.

Verify payment requests carefully.



Use only **official** app stores.

Enable **transaction alerts.**

Secure commerce = Customer Trust + Financial Safety.

UNIT 5: END-POINT & DEVICE SECURITY

End-Point: User-level devices (Laptops, Mobiles, IoT) connecting to network. Entry points for attacks.

Mobile Security

- Screen locks (PIN/Biometric).
- App permissions (Limit access).
- Download from trusted stores.

Password Policy

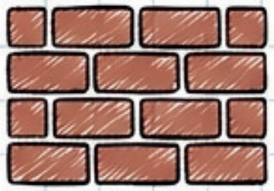
- Complex (Upper/Lower/Symbol/Number).
  - P@ssw0rd123!
- Regular changes & No reuse.
- **MFA:** Know (Password) + Have (OTP) + Are (Biometric).

Systems Management

- Patch Management: Update software to fix vulnerabilities.
- **Data Backup:** 3-2-1 Rule (Local/Cloud).
  - 3 copies
  - 2 media
  - 1 offsite
- Third-Party Software: Verify licenses.

NETWORK DEFENSE & CONCLUSION

Firewall



Barrier between internal & external network. Controls traffic.

Antivirus

Detects & removes malware. Needs updates.

Wi-Fi Security

Use WPA2/WPA3. Disable WPS. Strong passwords.

Cyber Hygiene: ➡ Regular updates, ➡ Secure browsing, ➡ Awareness.

Conclusion: End-point is the LAST line of defense. Technical controls must be supported by USER AWARENESS.