1. 🎯 **How Many Intelligence Gathering Disciplines Are There?**

There are **six core types of intelligence gathering disciplines**, often referred to by their abbreviations ending in "INT" (short for **intelligence**). These are the **main official disciplines** used across military, government, law enforcement, and cybersecurity.

🧠 **The 6 Primary INTs (Intelligence Disciplines)**

1. **OSINT** – *Open Source Intelligence*
   Information from public sources like websites, news, social media, etc.

2. **HUMINT** – *Human Intelligence*
   Information gathered directly from people (like interviews, informants, spies).

3. **SIGINT** – *Signals Intelligence*
   Info collected from communications (e.g., phone calls, emails, radio signals).

4. **GEOINT** – *Geospatial Intelligence*
   Info from maps, satellite images, GPS data—anything tied to location.

5. **MASINT** – *Measurement and Signature Intelligence*
   Highly technical data like radiation, sound waves, heat signatures, etc.

6. **CYBINT / TECHINT** – *Cyber Intelligence / Technical Intelligence*
   Info from the digital world: computer systems, networks, cyber

threats.

🔍 Other Related INTs (Sometimes Considered Subcategories or Extensions)

- **FININT** – *Financial Intelligence* (tracking money and transactions)
- **SOCMINT** – *Social Media Intelligence*
- **IMINT** – *Imagery Intelligence* (a part of GEOINT but sometimes listed separately)

💡 Summary for Your Slide

✅ **There are 6 main intelligence disciplines (INTs)**, and a few others that are more specialized.
Together, they help gather, analyze, and use information to make smarter decisions in everything from **national defense to cybersecurity to business strategy**.

2. INTs are different **categories or methods** used to **collect, analyze, and interpret information**. Each type of "INT" focuses on a different source or method of getting intelligence.

These are mostly used in **military, law enforcement, cybersecurity, and national defense**, but they are becoming more important in **business, disaster response, and even journalism**.

🌐 The 6 Core Intelligence Disciplines

Here are the most widely accepted and official INTs:

---

1. OSINT – Open Source Intelligence

- 📖 **What it is:** Information collected from **publicly available sources**.
- 📚 **Examples of sources:**
  - News articles
  - Social media posts
  - Blogs, websites
  - Public government reports
  - YouTube videos, podcasts
- ✅ **Why it matters:** OSINT is often the **easiest, cheapest, and fastest** way to get information—and it's legal. Many organizations rely on it for early warning signs or situational awareness.

---

2. HUMINT – Human Intelligence

- 🗣️ **What it is:** Intelligence gathered **from human sources**.

- 👤 **Examples:**
    - Interviews
    - Eyewitness accounts
    - Informants
    - Covert agents or spies
- ✅ **Why it matters:** HUMINT gives deep, personal insights—like intentions, emotions, or plans—that no machine or sensor can detect.

---

3. SIGINT – Signals Intelligence

- 📡 **What it is:** Information collected from **electronic signals or communications**.
- 📱 **Examples:**
    - Phone calls
    - Radio transmissions
    - Emails and text messages
    - Encrypted military communications
- ✅ **Why it matters:** SIGINT is crucial for intercepting hidden threats or understanding enemy strategies, especially in war or

cybersecurity.

---

4. GEOINT – Geospatial Intelligence

- 🌍 **What it is:** Information linked to **location and geography**.
- 🛰️ **Examples:**
    - Satellite images
    - Aerial drone footage
    - Maps and terrain models
- ✅ **Why it matters:** GEOINT is used in **military targeting, natural disaster response, tracking troop movements**, or even planning infrastructure.

---

5. MASINT – Measurement and Signature Intelligence

- 🔬 **What it is:** Intelligence gathered from **detecting and measuring physical phenomena**—things you can't see with the naked eye.
- 🌡️ **Examples:**
    - Heat radiation

    - Acoustic signals (e.g., submarine sonar)
    - Nuclear radiation
    - Chemical compositions
- ✅ **Why it matters:** MASINT is **highly technical** and used to detect **unusual or hidden activity** like nuclear weapons, stealth aircraft, or chemical leaks.

---

6. CYBINT (or TECHINT) – Cyber/Technical Intelligence

- 💻 **What it is:** Intelligence from the **digital and cyber world**.
- 🕵️ **Examples:**
    - Hacking attempts
    - Malware analysis
    - Tracking digital footprints
    - Analyzing computer networks
- ✅ **Why it matters:** In a digital world, CYBINT helps us **defend against cyberattacks**, understand hacker behavior, and protect sensitive data.

🧩 Other Commonly Mentioned INTs

These aren't always considered "core," but they're still useful:

Type	Description
FININT	Financial Intelligence – Tracking money, banking, and funding sources. Used in fraud, terrorism financing, etc.
SOCMINT	Social Media Intelligence – Specific form of OSINT that focuses only on platforms like Twitter, Facebook, Reddit.
IMINT	Imagery Intelligence – Often grouped with GEOINT, focuses strictly on interpreting images from satellites and drones.
DARKINT	Dark Web Intelligence – OSINT from hidden or hard-to-access parts of the internet.

📌 Summary Slide for Presentation

🔍 There are **6 main intelligence gathering disciplines**:
OSINT, HUMINT, SIGINT, GEOINT, MASINT, and CYBINT.
Each focuses on a different source — from people, to signals, to satellites — and together, they help governments, organizations, and companies **see more clearly and act more wisely**.

3.