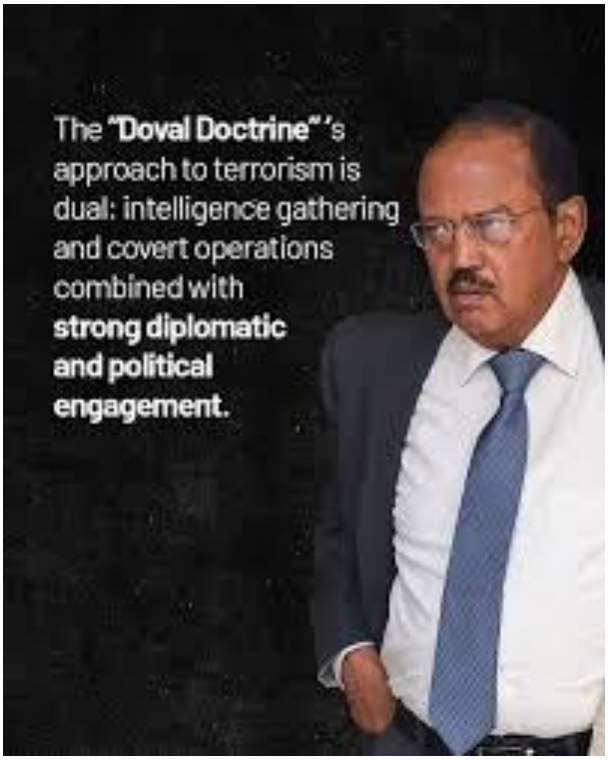
COVERT OPERATIONS AND NATIONAL SECURITY

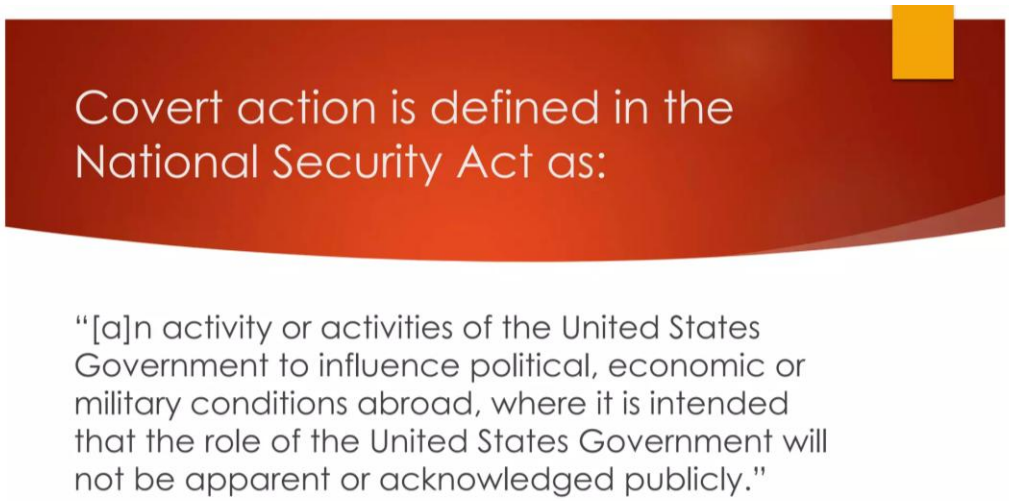
Context:

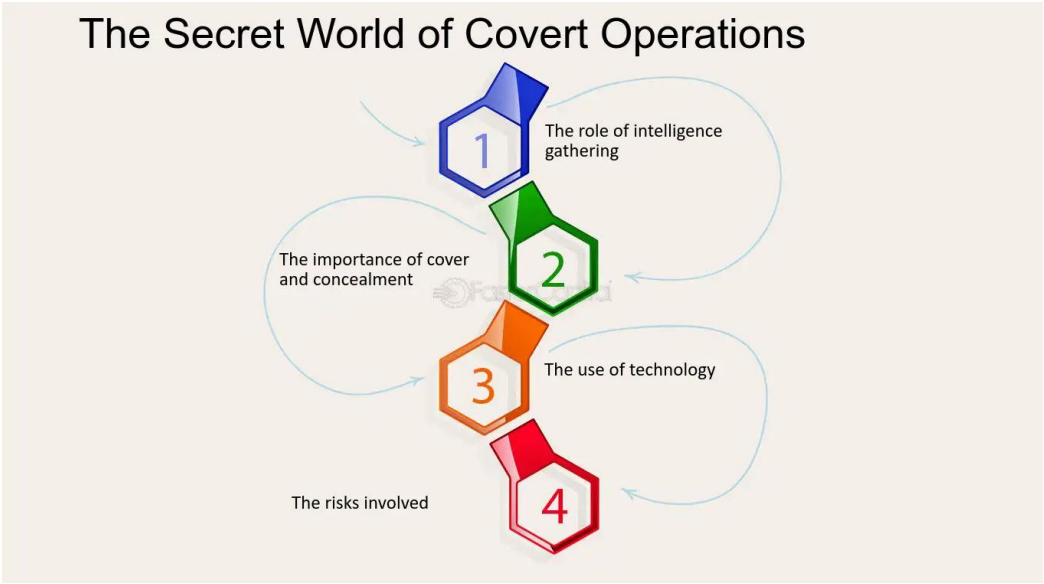


- Recently released **Dhurandhar movie follows a decade-long Indian intelligence covert operation which depicts the technicalities of the decade-long covert intelligence operation at its core**.

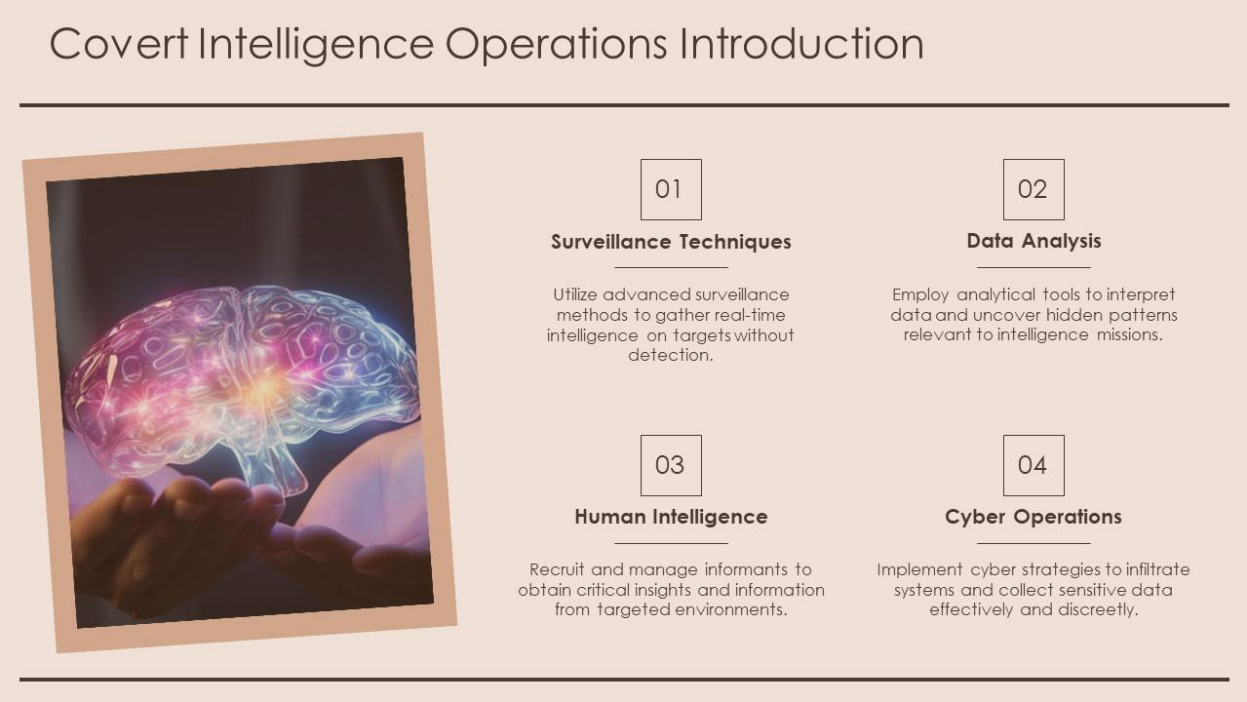
What are Covert Operations?

A covert operation is a secret mission, often by a government or intelligence agency, planned to hide the sponsor's identity and allow for plausible deniability, involving activities like espionage, sabotage, or influencing foreign politics without public acknowledgment, using methods like undercover agents, informants, or propaganda.





- **Covert action** can broadly be defined as operations that seek to influence **political, economic, or military conditions** abroad without exposing or highlighting the **role of the state conducting them.**
    - The tools of **covert action range from direct action to sophisticated propaganda** and other **forms of political manipulation.**
    - Given the term **"covert" and the legal emphasis** on concealing the **hand of the state**, it is easy to assume **plausible deniability is the essence of covert actions.**
    - However, a focus on **secrecy alone is misleading.**

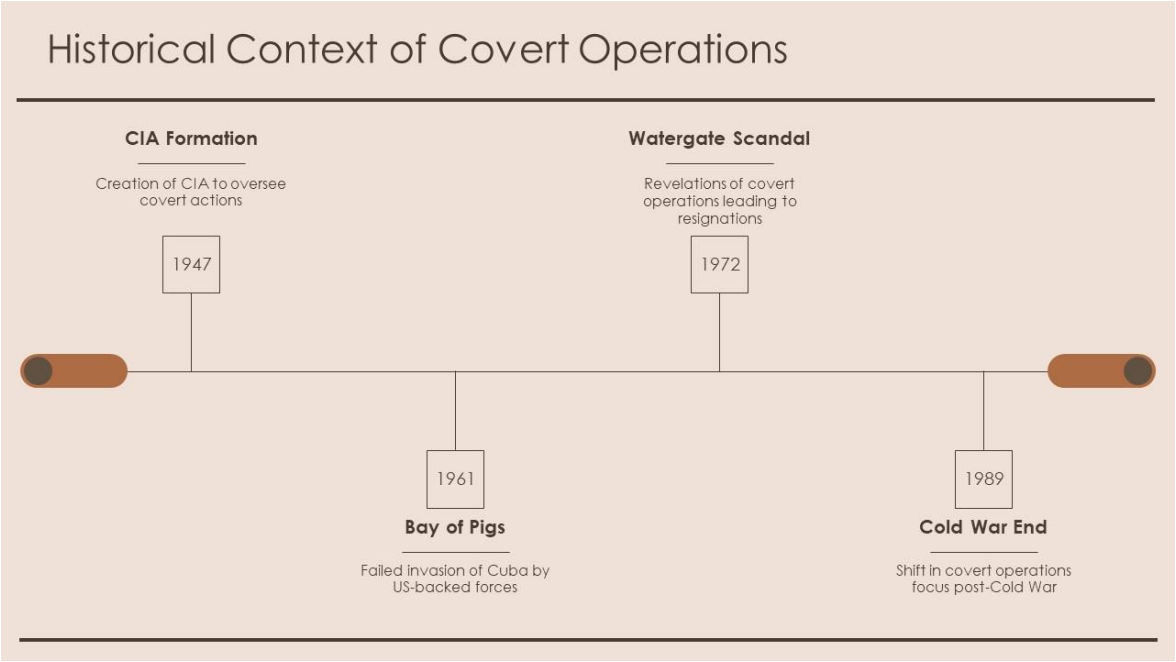


- Because of the **multiplicity of forms** that covert operations can take, it is difficult to **generally describe them.**
    - They occur in **both peace and war, and are used to influence and coerce friend, enemy, and neutral alike.**
- **Covert operations** give **policymakers an option to achieve** objectives when **disarmament** of the **enemy through direct military operations (or the threat of those operations) is undesirable.**

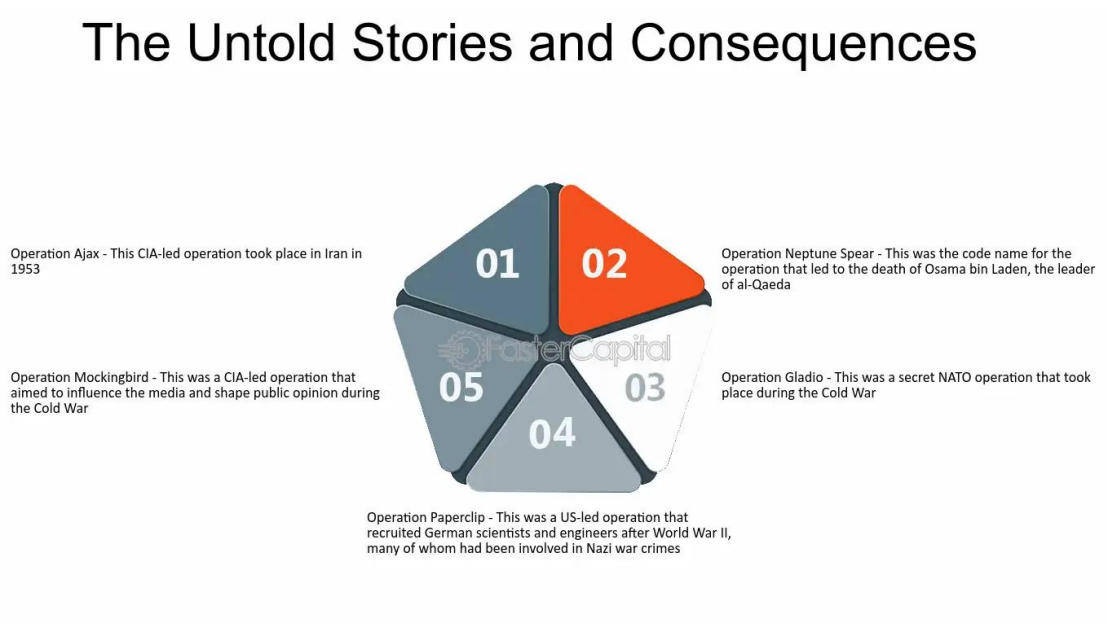
- **Covert operations** often fall short of **provoking a direct military response, or present enough ambiguity** to constrain a target state from **climbing to a higher "rung" of escalation dominance.**
- There are many situations when states cannot, **for political, material, or strategic reasons**, use their most prominent strengths to achieve policy goals.

- **Covert operations** are **similar to war in that they can decide major political issues.**
  - More **modest covert operations** can influence a state's **decision-making calculus.**

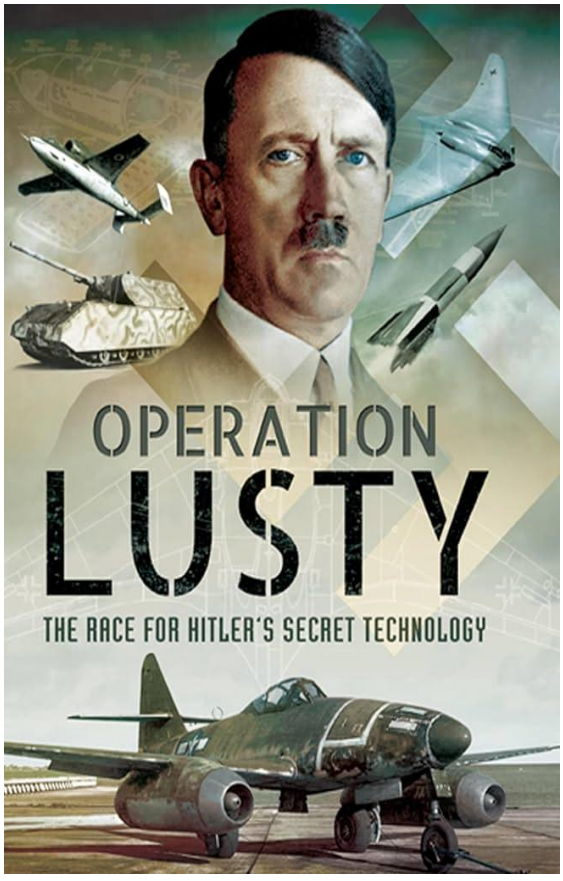
What is the historical context of Covert Operations?

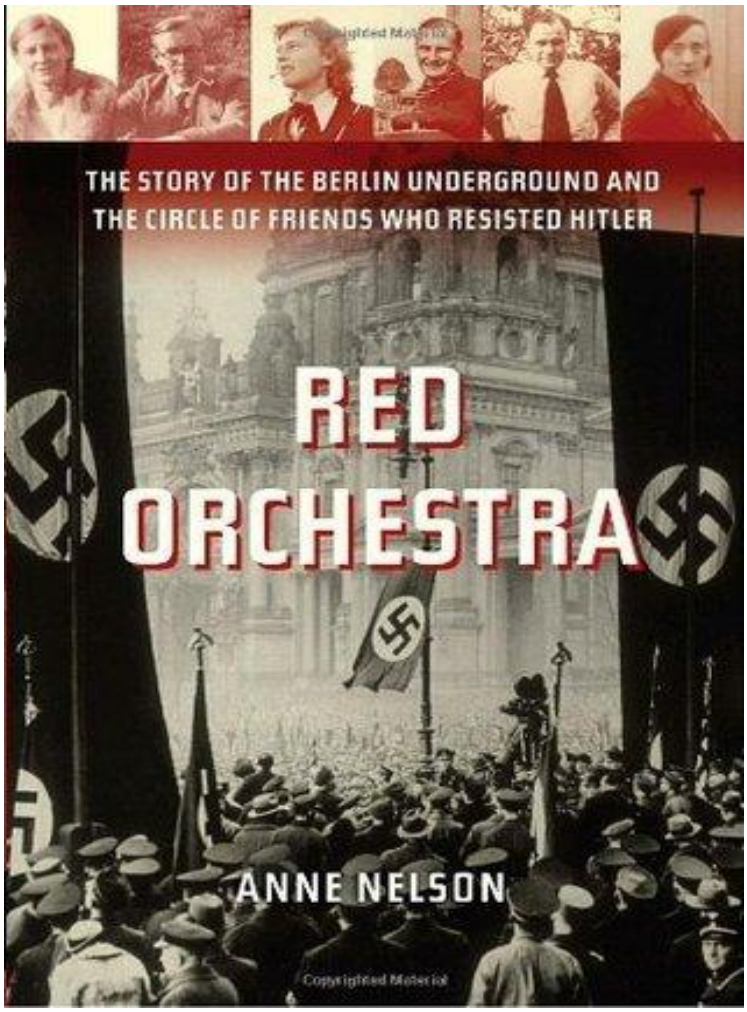
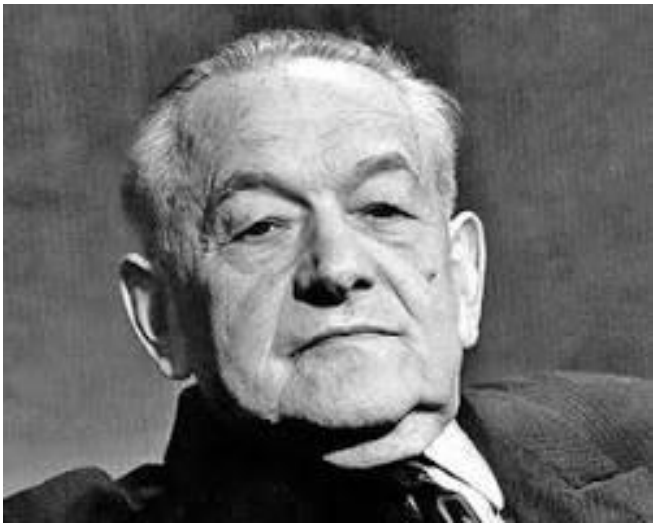


- The origin of modern covert operations traces to early **19th-century France with Eugène François Vidocq's police unit**, but the **concept as a major tool of statecraft** emerged in the **post-WWII Cold War**, driven by **US fears of Soviet influence**, with **George Kennan** and the **CIA formalizing these secretive actions** to influence foreign affairs without public acknowledgment.

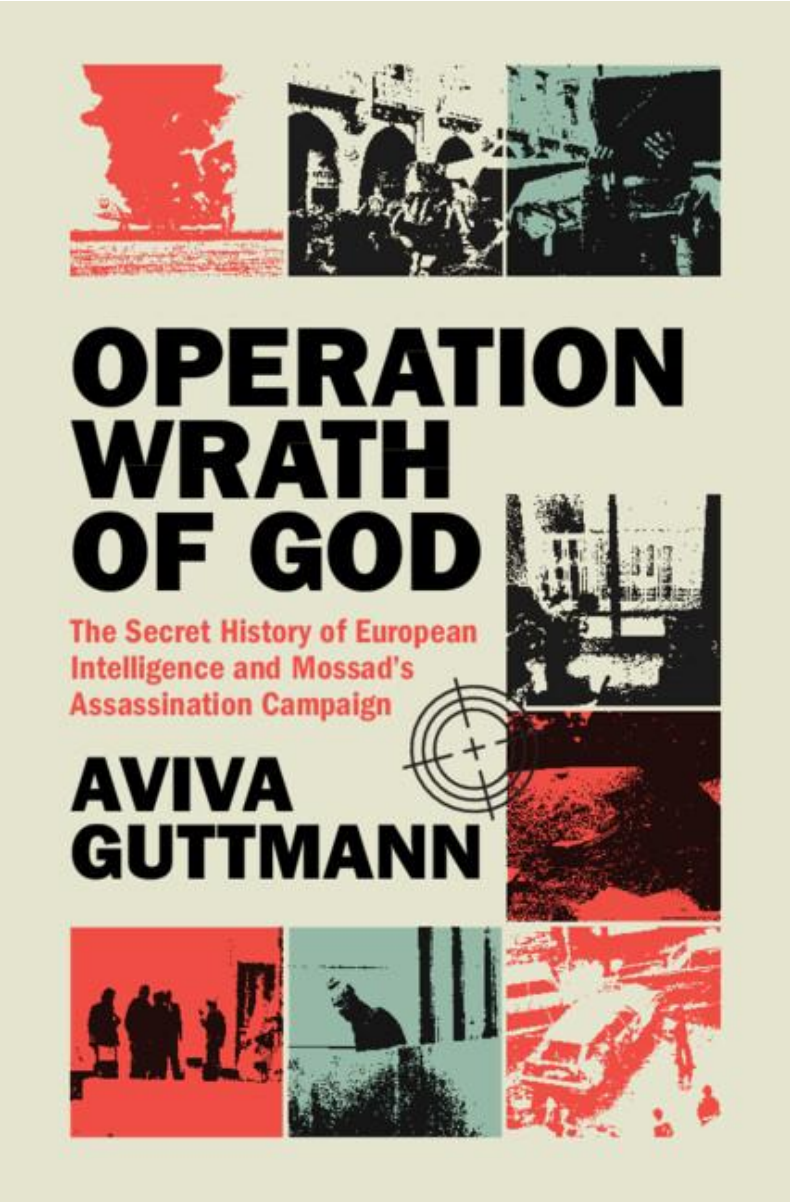


Enlist a few successful covert operations conducted globally

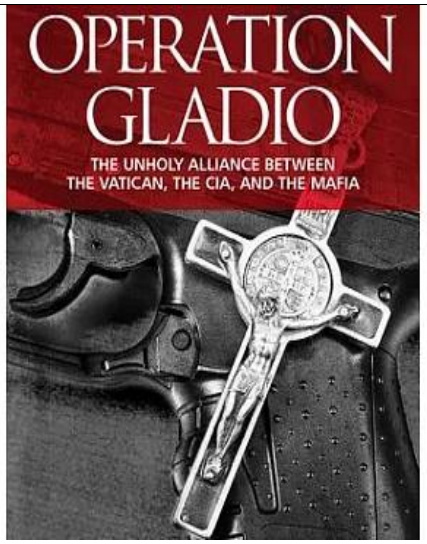
Operation	Description
Operation LUSTY	• It was a **post-World War II initiative** led by the **U.S. Air Force** to **seize** and analyze advanced **German military innovation**. • To **locate, recover, and study captured** German aircraft, weapons, and scientific documents. • Spearheaded by **Colonel Harold E. Watson** and the Air Technical Intelligence (ATI) teams. • Teams utilized **"Black Lists"** compiled during the war to identify high-priority enemy systems. • The operation **recovered 16,280 items**, totaling approximately 6,200 tons of equipment for shipment to the United States. • This operation played a **critical role** in **transferring advanced German aeronautical knowledge to the U.S.**, significantly influencing post-war aviation and defense technology. 

The Red Orchestra (Rote Kapelle)	 ● The Red Orchestra was a widespread network of **communist spies and resistance fighters** who operated against the Nazi regime during World War II. ● Founded and led by **Leopold Trepper**, a Polish-born communist, starting in the mid-1930s. 

	• The network established **"rings" across Nazi-occupied Europe**, including France, Belgium, and Holland, as well as neutral Switzerland. • To **gather military secrets for the Soviet Union** and act as an internal resistance force within German-occupied territories. • The group successfully **infiltrated Nazi offices** and obtained advanced documents regarding the invasion of the Soviet Union. • Despite the high quality of their intelligence, their warnings were **famously ignored** by the Soviet government.
Operation Gunnerside	• Operation Gunnerside was a high-stakes **sabotage mission** carried out by Norwegian commandos to disrupt Nazi Germany's nuclear ambitions. • On February 27, 1943, **nine Norwegian commandos successfully raided** the Vemork **hydroelectric plant in Rjukan**, Norway, destroying critical basement water pipes. • The **facility produced heavy water** (deuterium oxide), a vital component used by **German** scientists as a moderator to sustain **nuclear chain reactions.** • The sabotage significantly hindered Germany's progress toward developing an **atomic bomb.**

Operation Wrath of God	● Also known as **Operation Bayonet** was a covert assassination campaign authorized by Israeli Prime Minister Golda Meir and carried out by the Mossad.  ● The objective is to eliminate members of the **Palestinian terrorist group** Black September and the PLO who were believed to be responsible for the 1972 Munich Massacre, where 11 Israeli Olympic athletes were murdered. ● The operation lasted over 20 years, featuring high-profile hits across Europe and the Middle East using specialized teams.

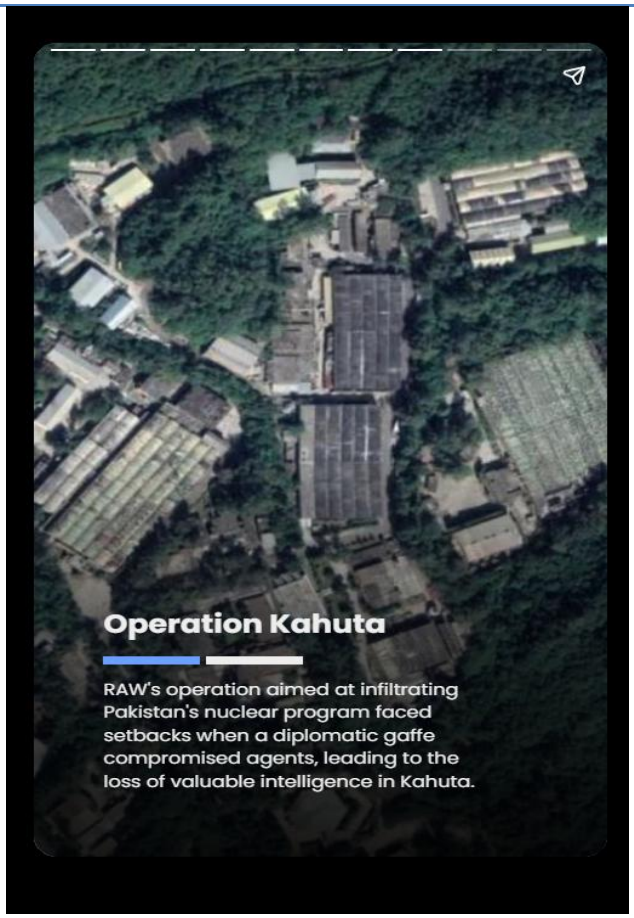
	• **The Lillehammer Affair**- The mission faced international backlash in 1973 after Mossad agents mistakenly assassinated an innocent Moroccan waiter in Norway, thinking he was the mastermind **Ali Hassan Salameh**.
Operation Washtub	• Operation Washtub was a top-secret **"stay-behind" program developed** during the early Cold War to prepare for a potential Soviet invasion of the United States. • Primarily focused on the **Territory of Alaska.** • The FBI and the Air Force Office of Special Investigations (OSI) recruited and trained local civilians—such as fishermen, trappers, and bush pilots—to act as secret agents. • If the **Soviets occupied Alaska**, these "stay-behind" agents were to hide in the wilderness, use secret survival caches, and transmit intelligence on enemy movements back to the U.S. mainland. • **A separate CIA operation** of the same name was used in 1954 to plant fake Soviet arms in Nicaragua to discredit the **Guatemalan government.**
Operation Gladio	• Operation Gladio was the **codename for a clandestine "stay-behind" network** organized by NATO, the CIA, and MI6 throughout Western Europe during the Cold War.

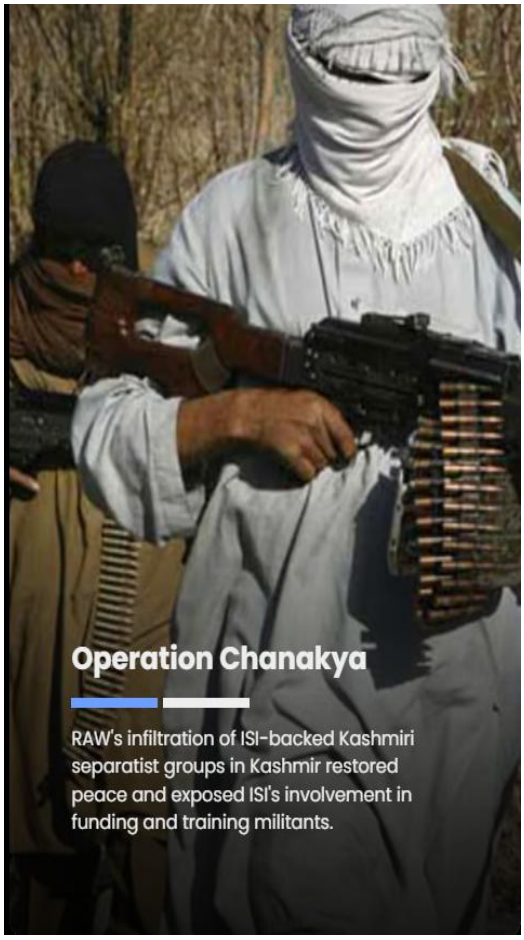


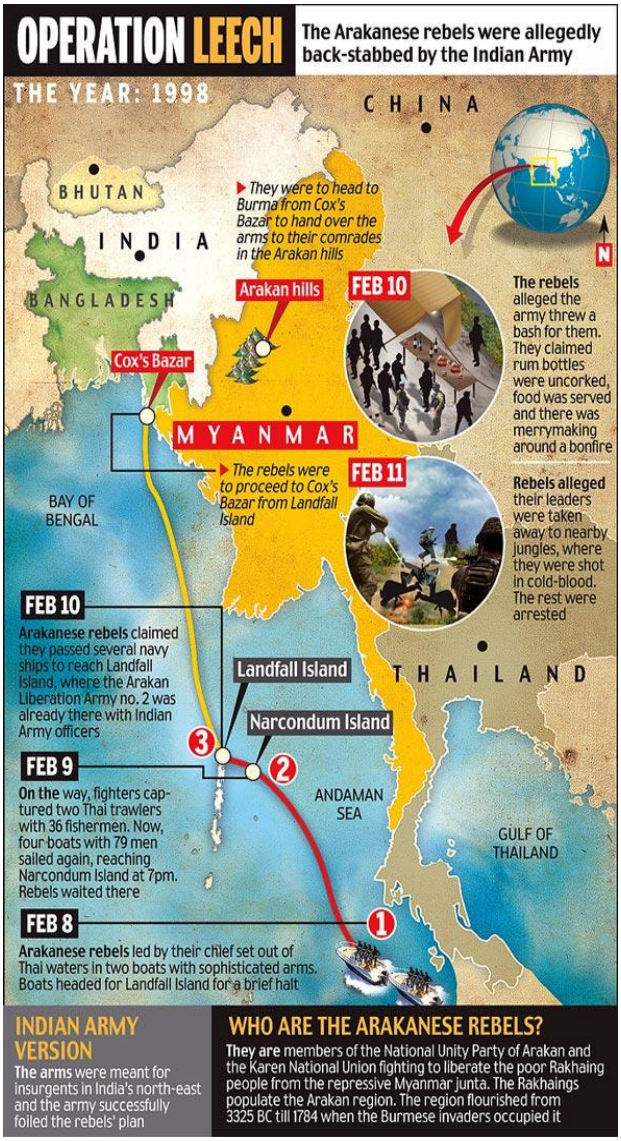
- To establish a **secret paramilitary resistance** that could operate behind enemy lines in the event of a Soviet invasion of Europe.
- It involved **secret arms caches,** underground bunkers, and trained civilian cells in countries like Italy, France, Germany, and Greece.
- In the 1990s, it was revealed that some branches of Gladio (particularly in Italy) became entangled in domestic politics, allegedly linked to right-wing terrorism and **"the strategy of tension"** to prevent left-wing parties from gaining power.

Mention some key operations of R&AW

Operation	Description
Operation Kahuta	• The operation was initiated by R&AW to get the **blueprints of Long-range nuclear missiles** from Pakistan's major nuclear weapons laboratory. • KRL is located in a small town called **Kahuta in the Rawalpindi district** of the Punjab Province, Pakistan. • The R&AW agents made thorough research & one of the brilliant prudent moves was the **extraction and testing of the hair samples** collected from the barbershops where the nuclear scientists used to get a haircut and that was nearby the Kahuta Nuclear facility. • The **traces of plutonium radiation in hair samples** pointed out that something was going on. Although the RAW was working vigorously things changed after the fall of Indira Gandhi in the 1977 elections which led to Morarji Desai being elected as the PM. • **Morarji Desai thwarted the operation** as by mistake he tipped about the RAW **agents' presence in Pakistan to General Zia Ul Haq**. All the RAW agents in Pakistan were brought down by Pakistan and that was the end of Operation Khahuta. • However, It is believed that India wanted **to bomb the Kahuta plant with help from Israel**, who according to reports, wanted to **use Gujarat's Jamnagar base** to launch its jets and another base for refueling. • In March 1984, Indira Gandhi gave a **green signal to the operation**, bringing India, Pakistan, and Israel within striking distance of a nuclear conflict. But it never happened.

	
Operation Smiling Buddha (Pokhran-I)	• On May 18, 1974, India successfully conducted its **first nuclear weapon test,** codenamed "Smiling Buddha." This event marked a significant turning point in global geopolitics and India's status as a scientific power. • A **plutonium-based** implosion device with an explosive yield of approximately 15 kilotons. • The **Pokhran Test Range (PTR)** in the **Thar Desert, Rajasthan**, located on a remote **Indian Army base.** • The **Research and Analysis Wing (R&AW)** was tasked with maintaining extreme secrecy. • Notably, this was the **first time R&AW traditionally an external intelligence agency, was assigned a high-priority domestic security mission**. • The successful detonation caught the world's most prominent intelligence agencies **completely off**

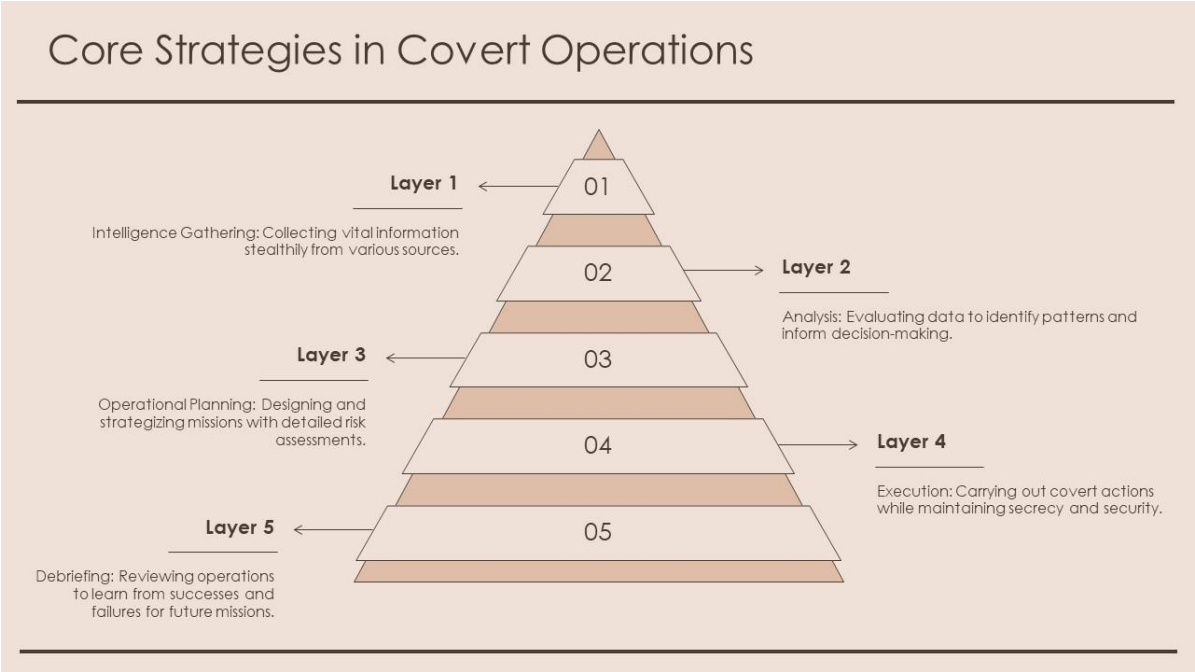
	guard. Agencies including the **CIA (USA), MSS (China), and ISI (Pakistan)** failed to detect the preparations, leading to a massive shift in **international relations and nuclear policy.**
Operation Chanakya	• **Operation Chanakya was the operation started by RAW** in the Kashmir valley to **kill and arrest various ISI-backed Kashmiri separatist groups** and restore peace in the Kashmir valley. • R&AW operatives raided various complexes and collected military intelligence, gathered evidence about **ISI's involvement in training and funding Kashmiri separatist** groups that work against India.  • RAW also got success in unearthing the links between **The Inter-Services Intelligence (ISI)** and militants RAW is also credited for creating a split in the **Hizb-ul-Mujahideen.**

	● **Operation Chanakya** also marked the **creation of pro-Indian groups** in Kashmir named **Ikhwan-ul-Muslimeen**, Muslim Mujahideen, etc. ● Ikhwan-ul-Muslimeen leader Kokka Parrey was **himself assassinated by separatists militants** which were backed by ISI.
Operation Leech	 ● The relationship between **Indian intelligence and Myanmar's rebel factions** is a complex case study in shifting strategic interests. What began as a **partnership to install a pro-democracy government** eventually culminated in a **lethal crackdown** known as Operation Leech.

	• **Myanmar was always a tricky area for Indian intelligence.** • Especially because of the dense forests being surrounded by the **Arakan's (ethnic people of Myanmar).** • India wanted to **promote democracy** in **Myanmar** and help put a friendly government in the region. • For this, R&AW established and funded **Burmese rebel groups** and pro-democracy parties in the region, like the **Kachin Independence Army (KIA).** • India gave permission to KIA to carry out trade in **jade and precious stones.** They even gave out weapons to them. • But when relations with KIA turned sour and they started **providing training ammunition to north-eastern rebel groups**, then RAW initiated **Operation Leech.** • Their mission was to **assassinate** the **Burmese rebel leaders** as an example for other rebel groups that conspired against the welfare of **Myanmar and India.** • In 1998, **six top rebel leaders were shot dead** and several others were jailed on charges **of gun-running in the country.**
Khalistan Movement	• The **Khalistan movement is a Sikh separatist movement** seeking to create a homeland for **Sikhs KHALISTAN (LAND OF KHALSA).** • Back in the mid-1980s **backed by ISI,** the Khalistan militancy was at its peak then R&AW decided to **set-up two covert task forces** to counter the militants in Punjab named **CIT-X and CIT-J** was supposed to counter the militants and the Khalistani groups.

	• R&AW not only managed to **flush out all the militants** and but they also destabilized certain parts of **Punjab on the Pakistani** side eventually forcing ISI to retreat and end all the activities

Mention core strategies opted in Covert Operations

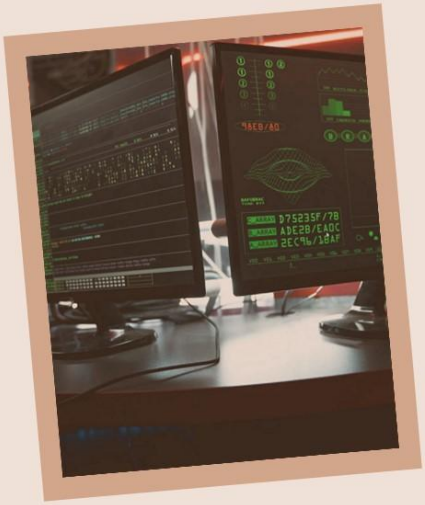


How does Covert Operations differ from Overt Operations?

	Covert Operations	Overt Operations	Covert Operations	Overt Operations
Definition	Text Here	Text Here	Text Here	Text Here
Purpose	Text Here	Text Here	Text Here	Text Here
Examples	Text Here	Text Here	Text Here	Text Here
Risks	Text Here	Text Here	Text Here	Text Here

Mention Various Espionage Techniques and tactics adopted in Covert Operations?

Espionage Techniques and Tactics



Surveillance

Utilize discreet techniques for observing target movements and activities.

Human Intelligence

Recruit insiders to gain access to critical information and operational insights.

Technical Interception

Employ technology to tap communications and gather data covertly.

Cyber Operations

Launch attacks to infiltrate networks and extract sensitive information.

Deception Plans

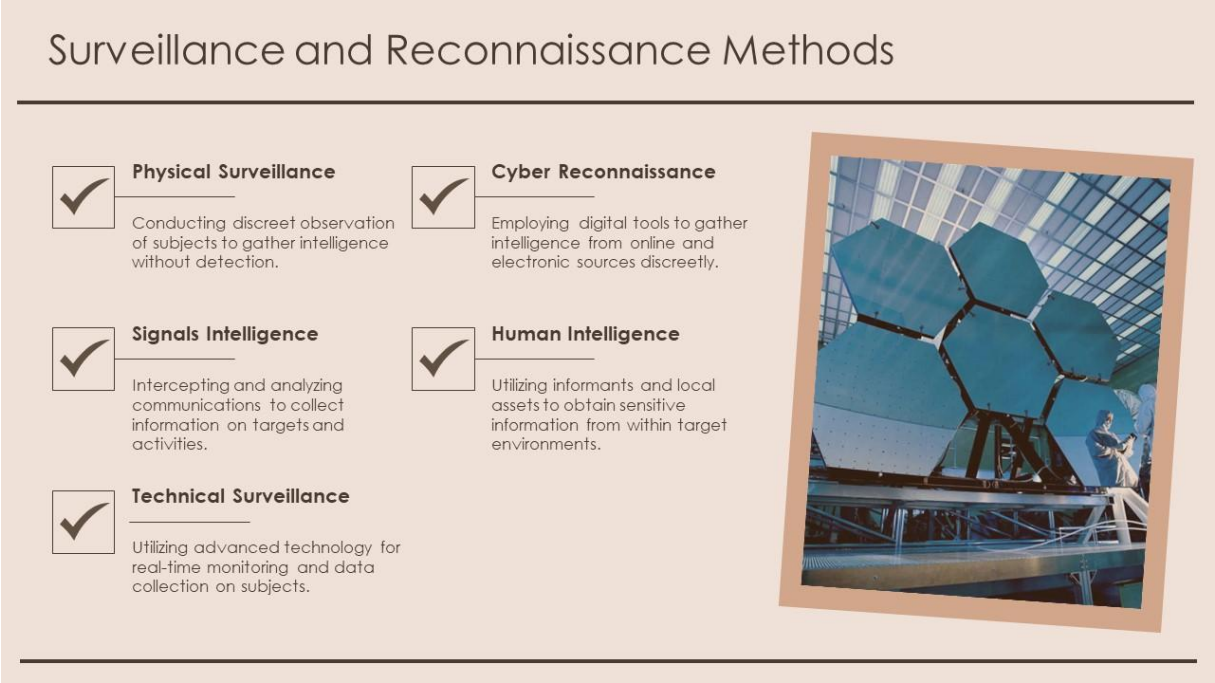
Implement strategies to mislead targets and manipulate their actions.

Techniques	Analysis
Human Intelligence (HUMINT): The Art of	• **Covert agents, or spies, are often on the frontlines of economic espionage.** • They use **HUMINT to gather vital information** through

Infiltration	human interaction. ● One classic example is the recruitment of insiders within a target organization. ● For instance, a **foreign intelligence agency** might convince an employee to **share proprietary information** in exchange for financial incentives, exploiting personal vulnerabilities, or even threatening exposure. ● The **notorious case of Robert Hanssen**, an FBI agent turned Russian spy, exemplifies the effectiveness of such infiltration tactics.
Cyber Espionage: The Digital Battlefield	● In today's **tech-driven world**, cyber espionage has become a prominent tool in the covert operative's arsenal. ● **State-sponsored hackers** and corporate entities engage in sophisticated cyberattacks to steal trade secrets, intellectual property, and sensitive data. ● The **Chinese hacking group known as APT10,** implicated in numerous corporate data breaches, demonstrates how nations can weaponize technology to gain economic advantages.
Social Engineering: Manipulating Human Behavior	● **Social engineering techniques** are employed to **manipulate individuals** into divulging confidential information. ● This can range from **spear-phishing emails** to more elaborate schemes. ● For example, a **disgruntled ex-employee** could **deceive colleagues** to obtain access to secure systems, as seen in the case of Kevin **Mitnick, a former hacker** who used these tactics to breach a multitude of corporate networks.
Wiretapping and Eavesdropping:	● **Covert operatives** may resort to **wiretapping and eavesdropping** to intercept sensitive communications.

Silent Surveillance	• The **Watergate scandal**, where members of the **Nixon administration** installed listening devices in the **Democratic National Committee's headquarters**, highlights the **lengths to which even governments** may go to obtain economic and political intelligence.
Corporate Espionage: Unseen Competitors	• In the **corporate realm, companies** engage in covert operations against their rivals. • **Spies posing as employees,** moles placed within competitor organizations, and even sophisticated malware designed to infiltrate the competition's networks are all part of this **cloak-and-dagger game.** • The battle between **Uber and Lyft** for **ride-sharing supremacy witnessed allegations** of corporate espionage and trade secret theft.
Double Agents and Deception: The Web of Lies	• Double agents, individuals who **feign loyalty to one party** while secretly working for another, **create a web of deception** that can confound both intelligence agencies and private entities. • The **story of Kim Philby, a British MI6 officer** who spied for the **Soviet Union during the Cold War**, is a classic example of **how double agents can manipulate trust** to further their covert agendas.
Deniable Plausible Deniability: The Art of Concealment	• **Covert operatives and intelligence** agencies often employ tactics that provide **"plausible deniability."** • The **2010 Stuxnet virus**, allegedly created by the U.S. And Israel, **to target Iran's nuclear facilities,** showcased the u**se of sophisticated malware** with built-in safeguards to protect the identities of the responsible parties.

Mention Various Surveillance and reconnaissance (ISR) methods adopted in Covert Operations?



- The use of surveillance in covert operations is a crucial aspect of breaking syndicates.
- Surveillance can be used in many ways, from tracking individuals to gathering intelligence.

How Surveillance is used	Analysis
Tracking individuals:	• The most common use of surveillance in covert operations is to track individuals. • This involves **following a suspect** and gathering information on their whereabouts, movements, and activities. • This information is then used to build a case against the suspect. • Tracking individuals can be done in several ways, including using **GPS tracking devices,** physical surveillance, and monitoring their electronic devices.

Gathering intelligence:	• Surveillance can also be used to **gather intelligence.** • This involves monitoring communication channels, such as phone calls and emails, to gather information about a **syndicate's activities.** • This **type of surveillance can provide valuable insights** into the inner workings of a syndicate, including who the key players are, how they communicate, and what their plans are.
Covert surveillance:	• **Covert surveillance** is used when it is not possible to track an individual openly. • This involves using techniques such as **hidden cameras and microphones** to gather information without the suspect's knowledge. • Covert surveillance can be particularly effective in cases where the **suspect is highly skilled** at detecting and evading surveillance.
social media monitoring:	• Social media has become an increasingly important tool in covert operations. • **Monitoring** social media accounts can provide valuable insights into a syndicate's activities, including who they are communicating with and what their plans are. • However, social media monitoring can also be challenging, as suspects may use **encrypted messaging apps** to communicate.
Automated surveillance:	• Automated surveillance **involves using software to monitor communication** channels and flag suspicious activity. • This can be particularly useful in cases where there is a **high volume of data** to sift through, as software can quickly identify patterns and anomalies. • However, automated surveillance **is not foolproof,** and there is always a risk of false positives.

Mention various Innovations Driving Covert Operations?

Innovations	Analysis
Surveillance Technology:	• One of the **most critical aspects of covert operations is surveillance.** • **Operatives rely** on advanced surveillance technology to **gather intelligence and monitor targets discreetly.**

	• Drones equipped with **high-resolution cameras** and **thermal imaging capabilities have become invaluable tools for covert operatives.** • These **unmanned aerial vehicles (UAVs)** provide real-time video feeds and can access **hard-to-reach areas, allowing operatives to gather crucial information without detection.**
Communication Systems:	• Effective communication is essential for the success of covert operations. Traditional methods, such as **radio communication,** have limitations in terms of range and security. • However, the **advent of encrypted messaging apps** and secure communication devices has revolutionized how operatives communicate in the field. • These devices offer **end-to-end encryption**, ensuring that **sensitive information remains secure** and out of the hands of adversaries.
Cyber Intelligence:	• In the digital age, **cyber intelligence** has become a vital component of covert operations. • Hackers and cyber operatives play a crucial role in gathering information, **infiltrating networks**, and **disrupting the activities of adversaries.** • By leveraging sophisticated hacking tools and techniques, these operatives can breach secure systems, gather intelligence, and **even manipulate data** to mislead their targets. • The ability to operate in the **virtual realm** has opened up new avenues for covert operations, **making cyber intelligence** a powerful tool in the arsenal of covert operatives.

Biometric Technology:	• Covert operatives often need to remain **unidentified** and maintain their cover in high-risk situations. • Biometric technology has emerged as a game-changer in this regard. • **facial recognition systems** and **fingerprint scanners** enable operatives to verify identities quickly and accurately, ensuring that only authorized individuals gain access to sensitive areas. • Additionally, biometric technology can be **used to track and monitor targets,** providing operatives with valuable information about their movements and activities.
Stealth Technology:	• The ability to **remain undetected** is the cornerstone of covert operations. • In recent years, **advancements in stealth technology** have provided operatives with new ways to stay hidden in plain sight. • From **camouflage materials** that blend seamlessly with the environment to **silent drones** that can fly undetected, these innovations have enhanced the effectiveness of covert operations. • For example, the **development of radar-absorbent materials** has significantly reduced the radar signature of aircraft, making them less detectable by enemy radar systems.

Mention various Counter Intelligence measures in Covert Operations?

Counterintelligence Measures Explained

Risk Assessment

Identify potential vulnerabilities and prioritize assets needing protection.

Surveillance Detection

Implement techniques to identify and counteract unwanted surveillance activities.

Operational Security

Develop protocols to protect sensitive information from unauthorized access.

Information Control

Establish strict access guidelines for sensitive documents and communications.

Insider Threat Mitigation

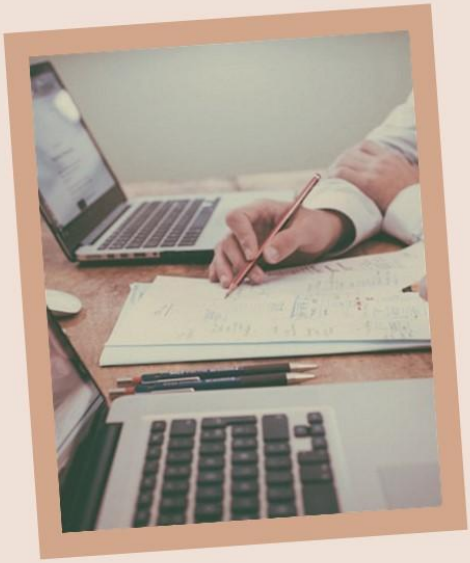
Regularly conduct background checks and monitor employee behavior for anomalies.

Cybersecurity Protocols

Employ advanced technologies to safeguard against digital espionage and attacks.

What are various Future trends of Covert operations?

Future Trends in Intelligence Operations



01

AI Integration

Leveraging artificial intelligence to enhance data analysis, automate surveillance processes, and predict threats in real-time, increasing operational efficiency and accuracy in intelligence gathering.

02

Cyber Operations

Expanding capabilities in cyber warfare tactics to protect assets, counter cyber threats, and gather intelligence through digital means, ensuring robust defense against espionage.

03

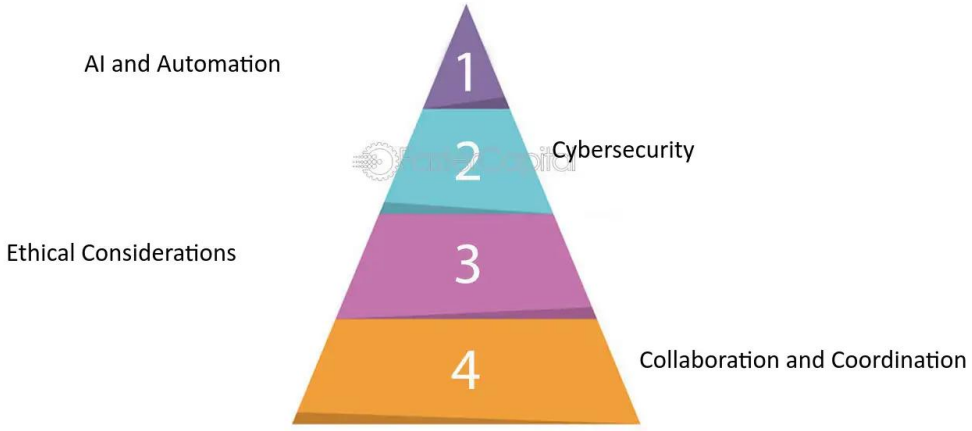
Open Source Intelligence

Harnessing publicly available information and social media platforms for intelligence analysis, improving situational awareness and enabling quicker decision-making in covert operations.

Future Trends	Analysis
AI and Automation	● AI and automation have the potential to revolutionize covert operations. ● With **machine learning algorithms**, intelligence agencies can analyze vast amounts of data **to identify patterns and trends** that may not be apparent to human analysts. ● This can lead to more effective and efficient operations, as well as better decision-making. For example, **AI-powered drones** can be used for surveillance and reconnaissance, reducing the risk to human operatives.
Cybersecurity	● As more covert operations involve the use of technology, cybersecurity becomes an increasingly **important concern.** ● Intelligence agencies must ensure that their systems are **secure and protected** from cyber attacks, which could compromise sensitive information or even put operatives at risk. ● This requires **constant vigilance** and the implementation of robust security protocols.
Ethical Considerations	● Covert operations have always raised **ethical questions**, and this is unlikely to change in the age of AI and big data. ● The use of advanced technology raises **new ethical dilemmas, s**uch as the use of autonomous weapons or the potential for AI to make decisions without human input. ● Intelligence agencies must carefully consider these **ethical considerations** and ensure that their operations are conducted in a manner that is consistent with their values and principles.

Collaboration and Coordination	• Covert operations often involve multiple agencies working together, and this will continue to be the case in the future. • However, the use of AI and **big data** will require even **greater collaboration and coordination**, as different agencies may have access to different data sets or utilize different technologies. • This requires effective **communication and information sharing**, as well as the development of common standards and protocols.

The Future of Covert Operations What Lies Ahead in the Age of AI and

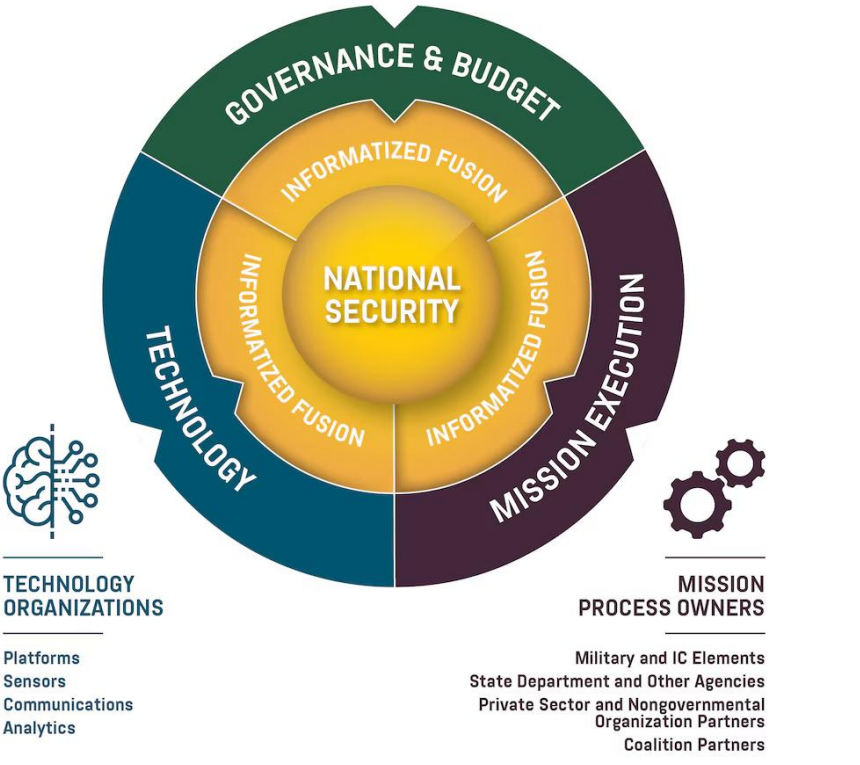


What is National Security?

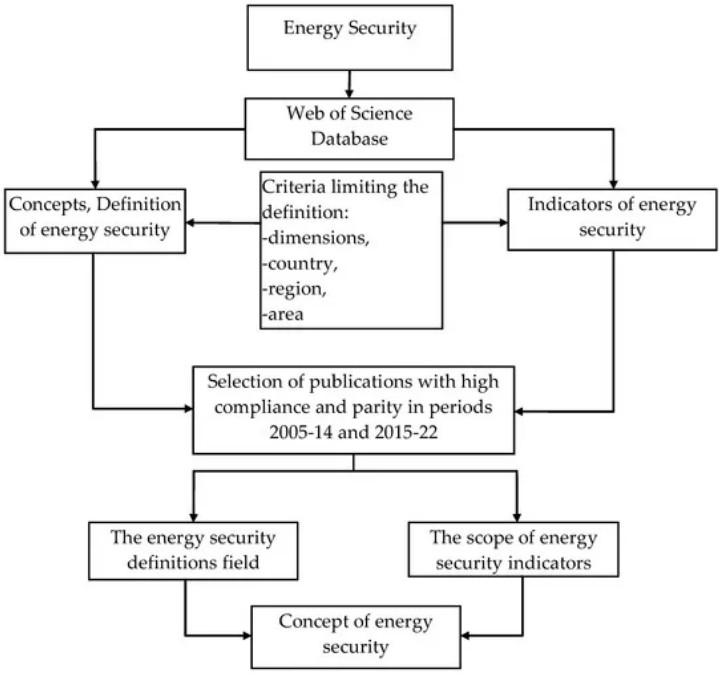
- **National security** has been described as the **ability of a state to cater for the protection and defence of its citizenry.**
- **India's national security** is a broad concept c**overing territorial integrity, economic stability, and technological resilience, facing threats from cross-border terrorism** (addressed via surgical strikes like in 2025's Operation Sindoor) and **internal challenges, requiring a modern, tech-driven approach** with agencies like the **NSG and strategies** leveraging **AI for future preparedness, managed by the National Security Council and National Security Advisor.**

Pillars of National Security	About
Multifaceted Strategy:	● Goes beyond military might to **include economic health, technological strength, internal harmony, and cyber resilience.**
Technology-Centric:	● Focus on **AI, data integration, and advanced system**s for **predictive security** and **future-proofing against evolving** threats.
Proactive Defence:	● Firm stance on **cross-border terrorism, demonstrated** by **surgical strikes in response to attacks.**

Mention various elements of National Security?



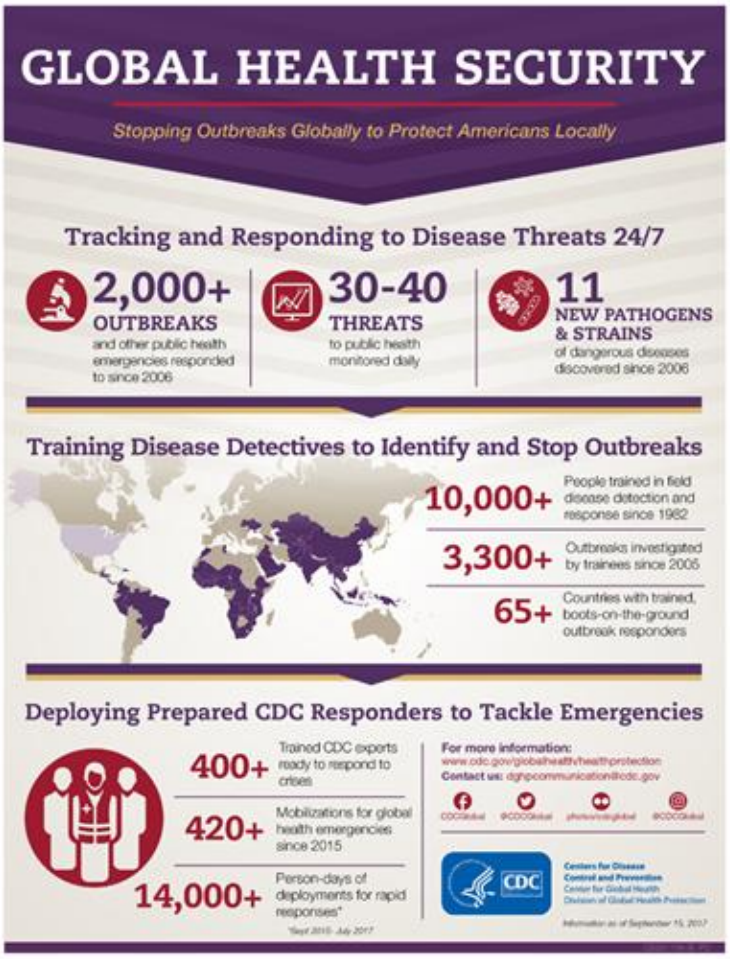
Elements of National Security	Analysis
Military Security:	• Protecting borders, sovereignty, and countering external threats through armed forces.
Economic Security:	• Ensuring national wealth, stable markets, and citizen economic freedom.

Political Security:	• Maintaining stable governance, rule of law, and strong institutions.
Energy Security:	• Securing uninterrupted energy supply and assets. 

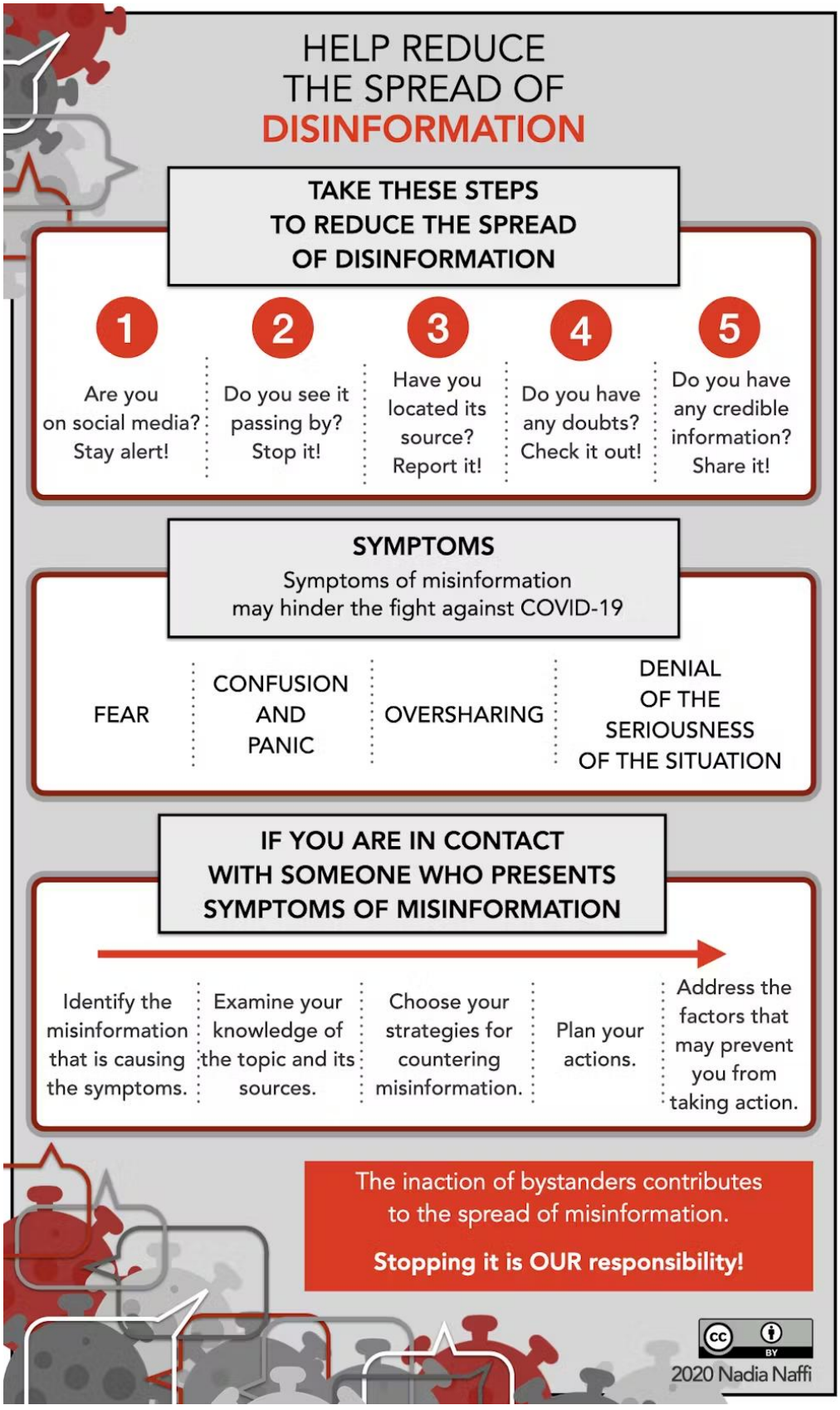
Food Security:	● Ensuring access to sufficient, nutritious food for the population.

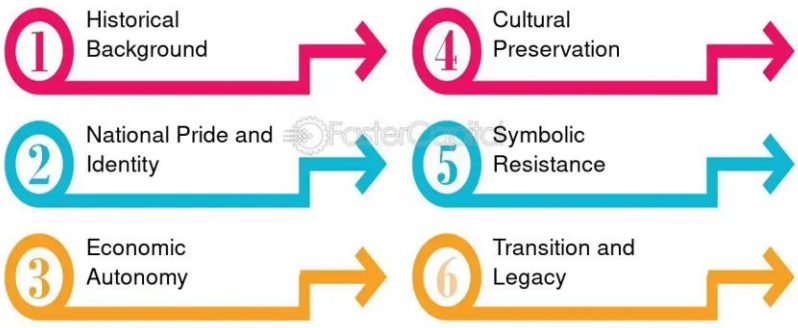
Cyber Security:	• Protecting digital infrastructure and data from attacks.
Environmental Security:	• Addressing climate change, natural disasters, and resource depletion.

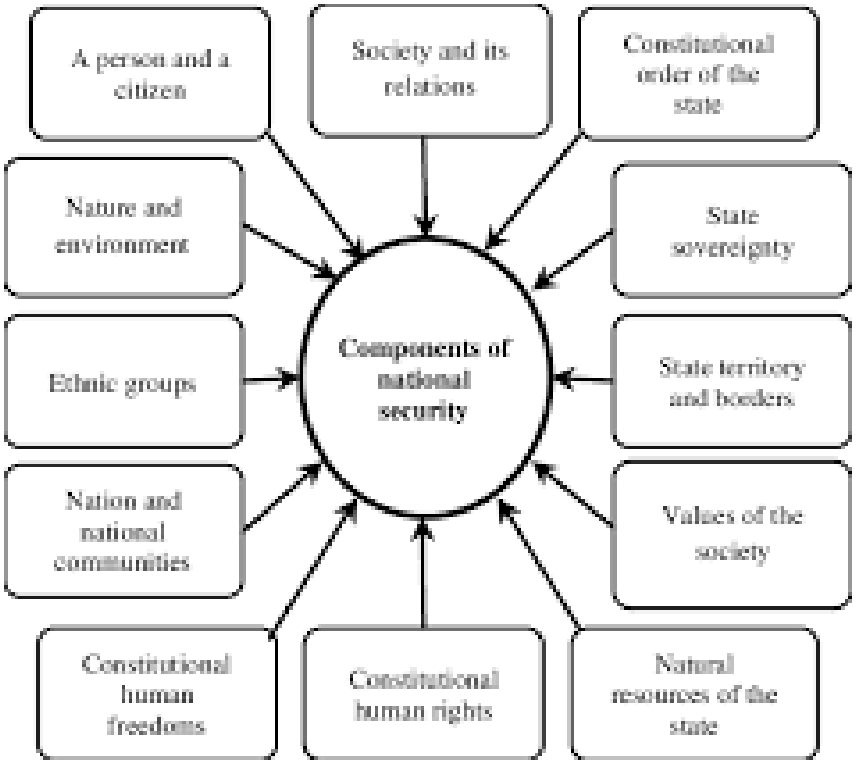
Health Security:	● Protecting public health from pandemics and other threats.



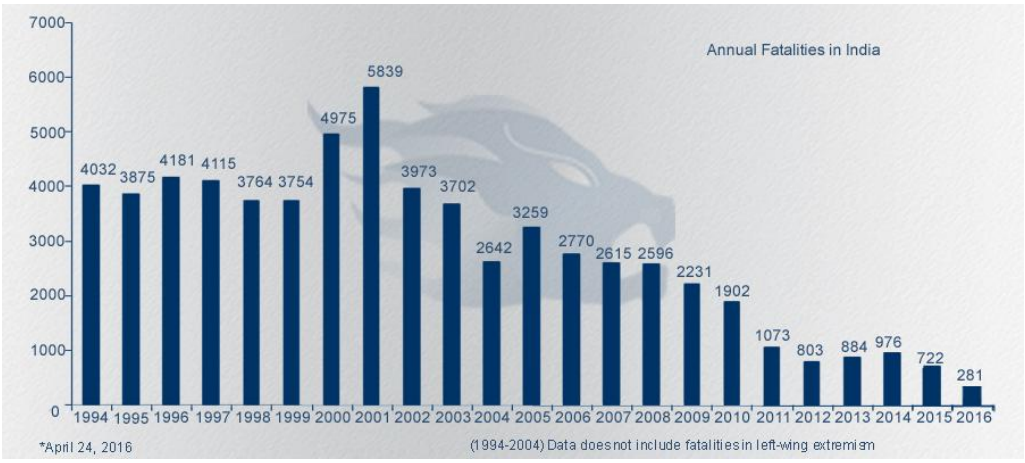
Information Security:	• Managing information flow and countering misinformation.

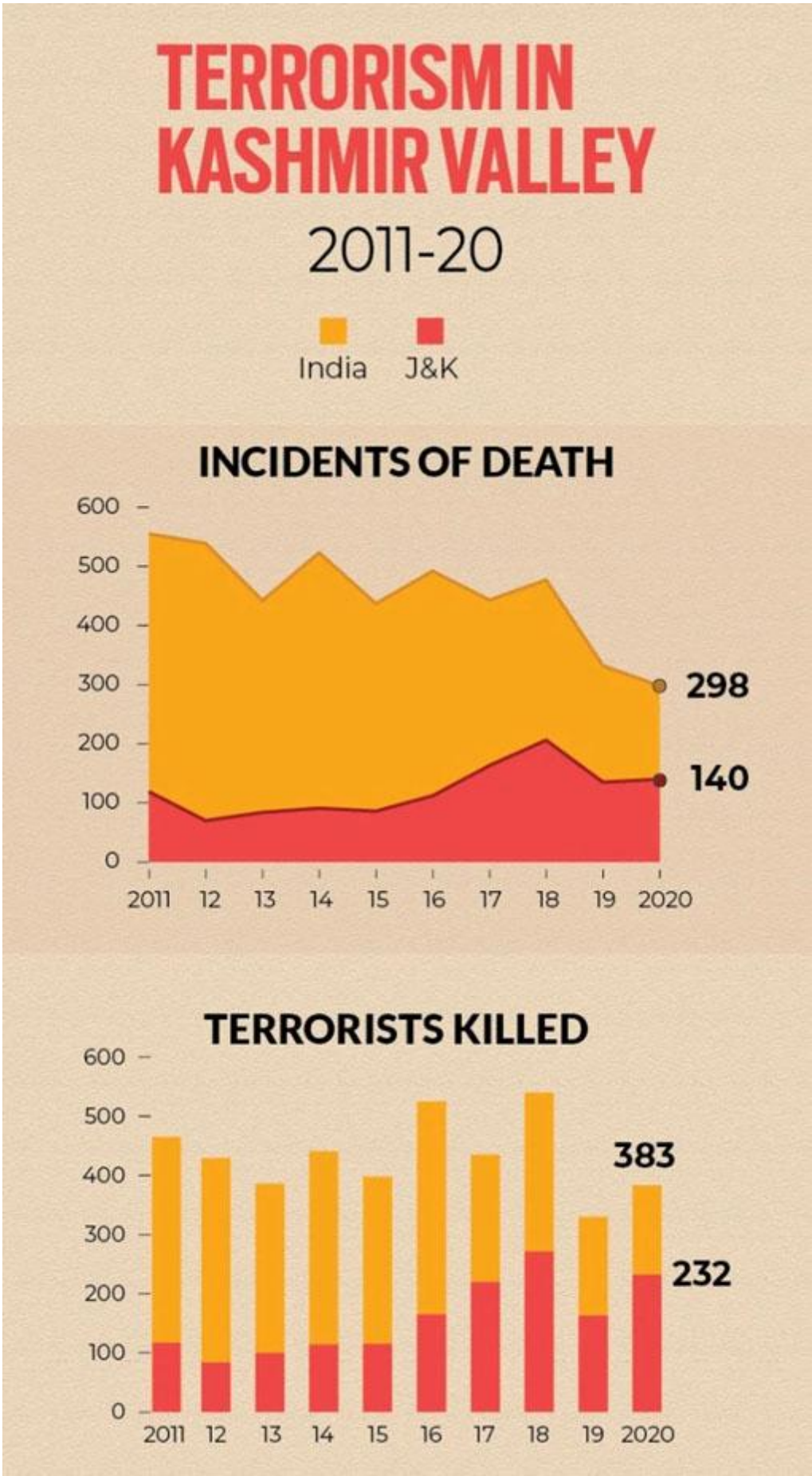


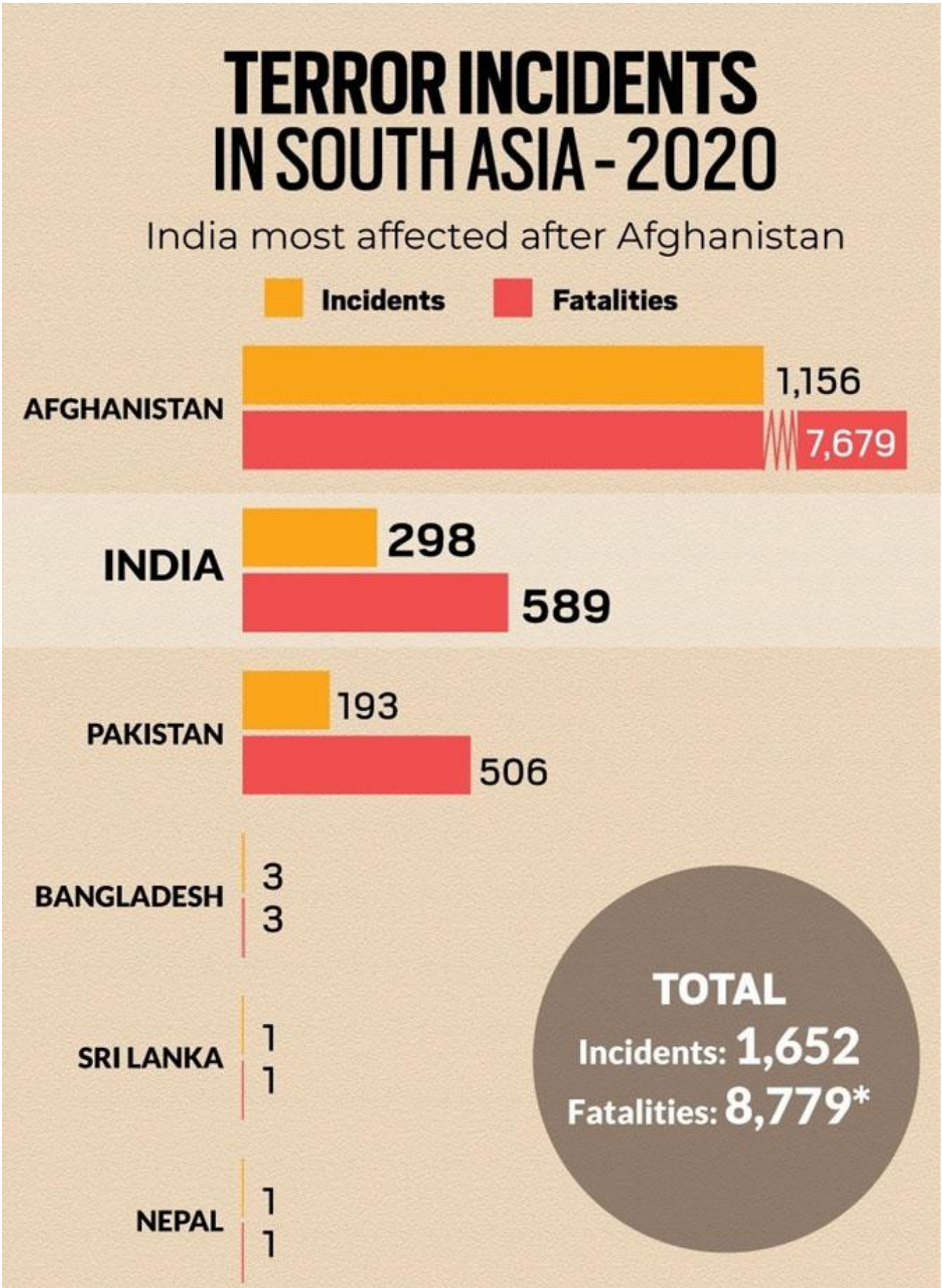
Cultural Security:	• Protecting national identity and values.
Diplomacy:	• Using non-military means to resolve conflicts and build alliances. **Instruments of National Power** **D** Diplomatic: Embassies/ Ambassadors; Recognition; Negotiations; Treaties; Policies; International forums **I** Informational: Military information; Public diplomacy; Public affairs; Communications resources; International forums; Spokespersons, timing, media and venues for announcements **M** Military: Military operations; Engagement, Security Coop, Deterrence; Show of force; Military technology; Size, composition of force **E** Economic: Trade policies; Fiscal and monetary policies; Embargoes; Tariffs; Assistance Symbol of National Identity 

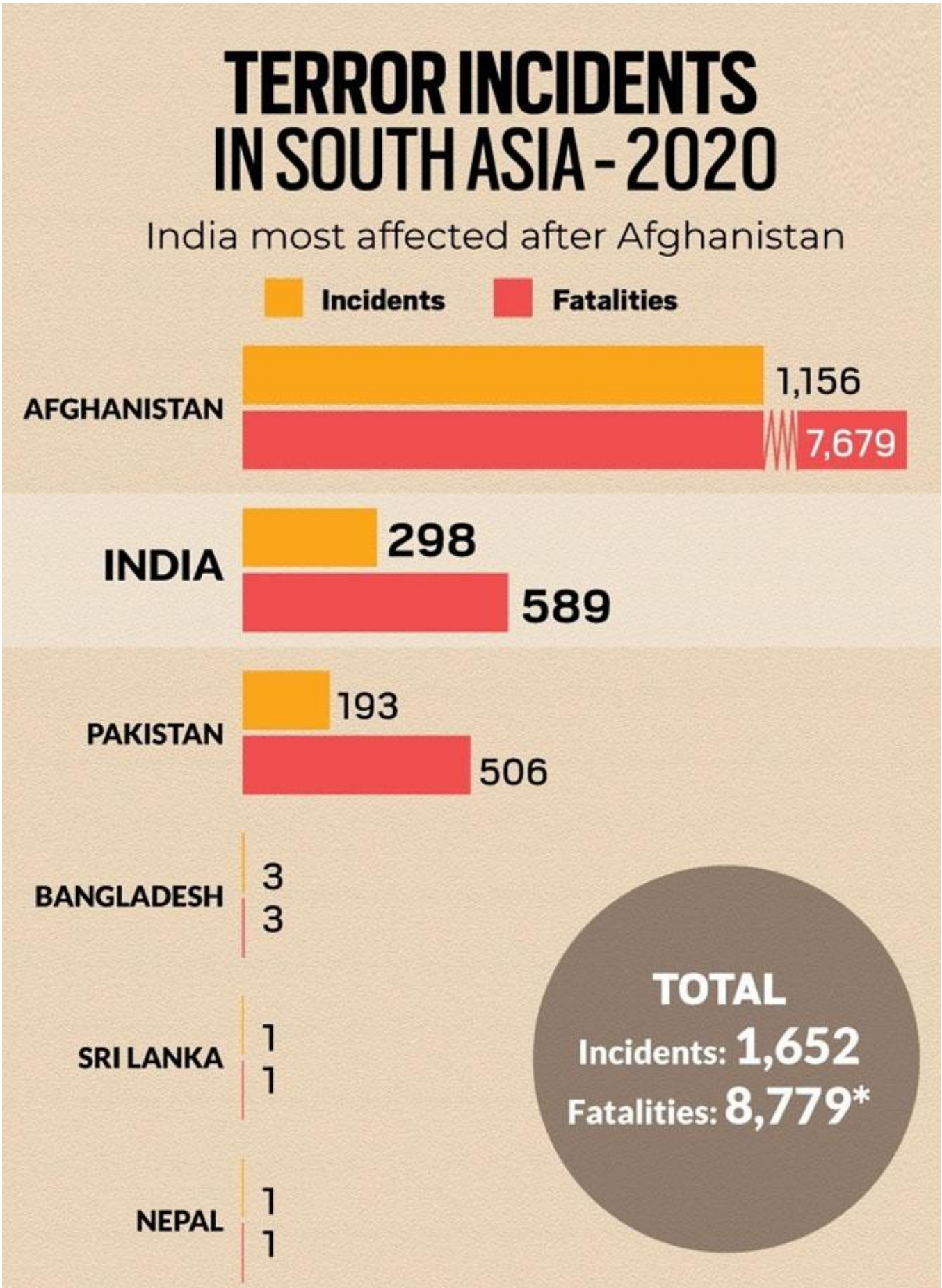


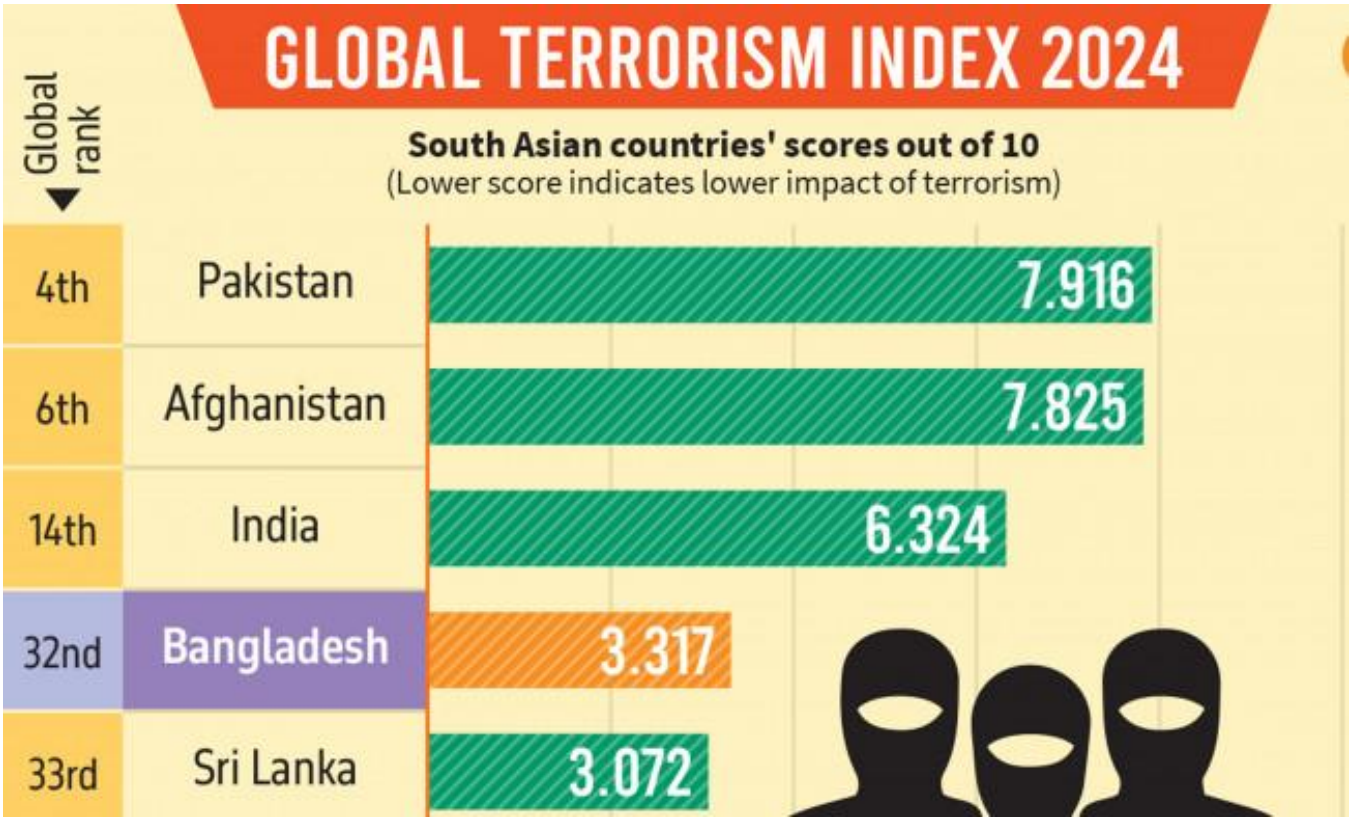
Enlist data on breach of national security in India?

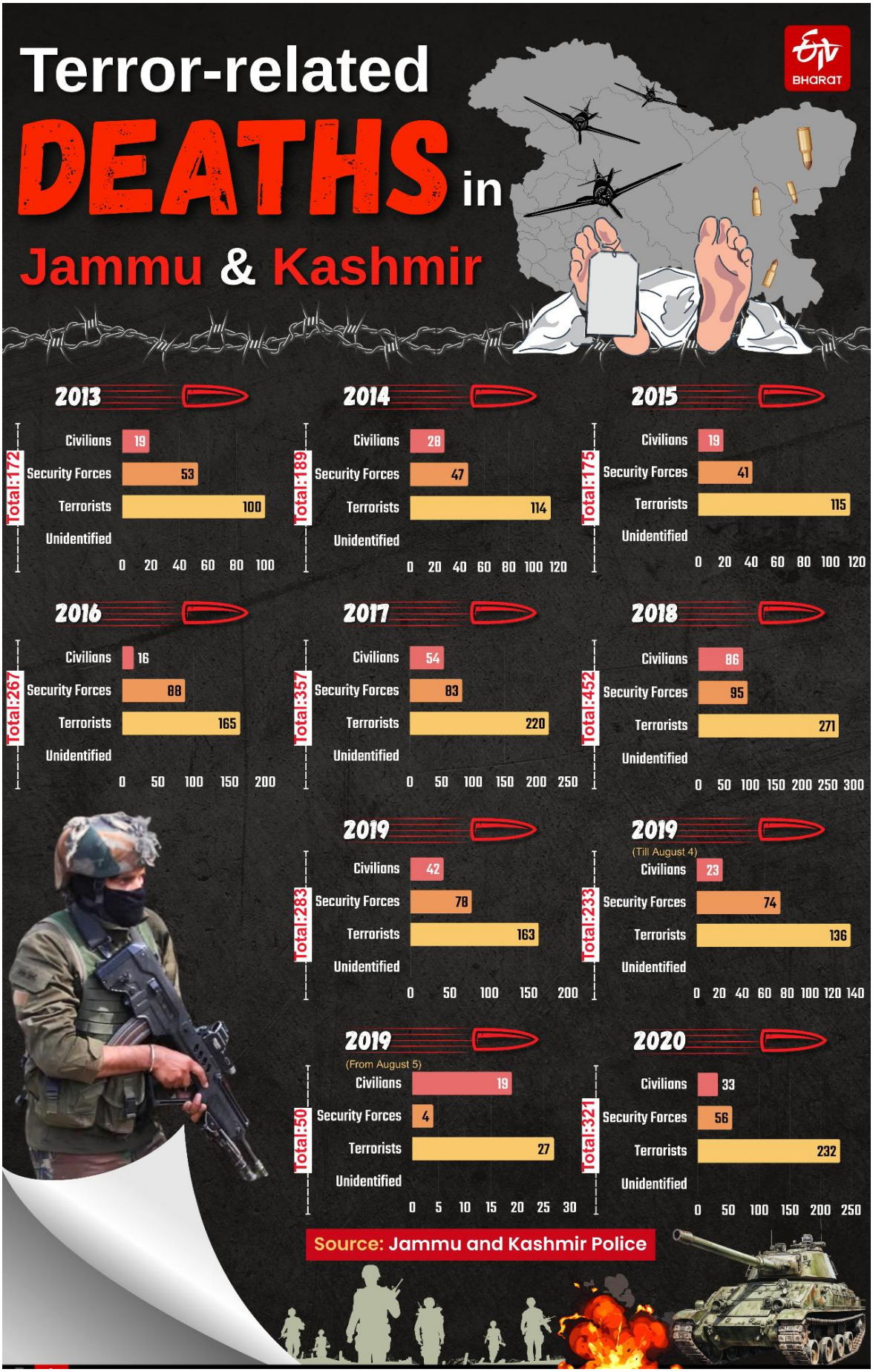



TERRORISM IN KASHMIR VALLEY
2011-20
India
J&K
INCIDENTS OF DEATH
600
500
400
300
200
100
0
2011
12
13
14
15
16
17
18
19
2020
298
140
TERRORISTS KILLED
600
500
400
300
200
100
0
2011
12
13
14
15
16
17
18
19
2020
383
232

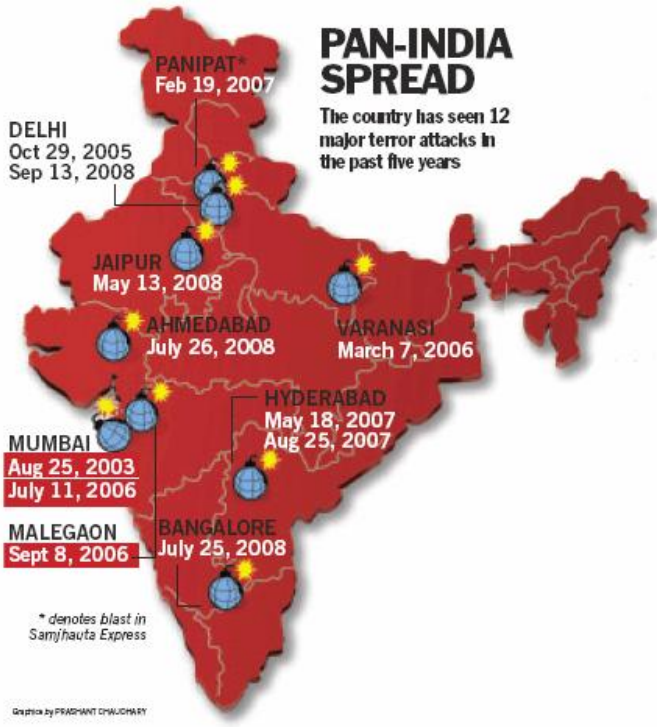

TERROR INCIDENTS IN SOUTH ASIA - 2020
India most affected after Afghanistan
Incidents
Fatalities
AFGHANISTAN
1,156
7,679
INDIA
298
589
PAKISTAN
193
506
BANGLADESH
3
3
SRI LANKA
1
1
NEPAL
1
1
TOTAL
Incidents: 1,652
Fatalities: 8,779*

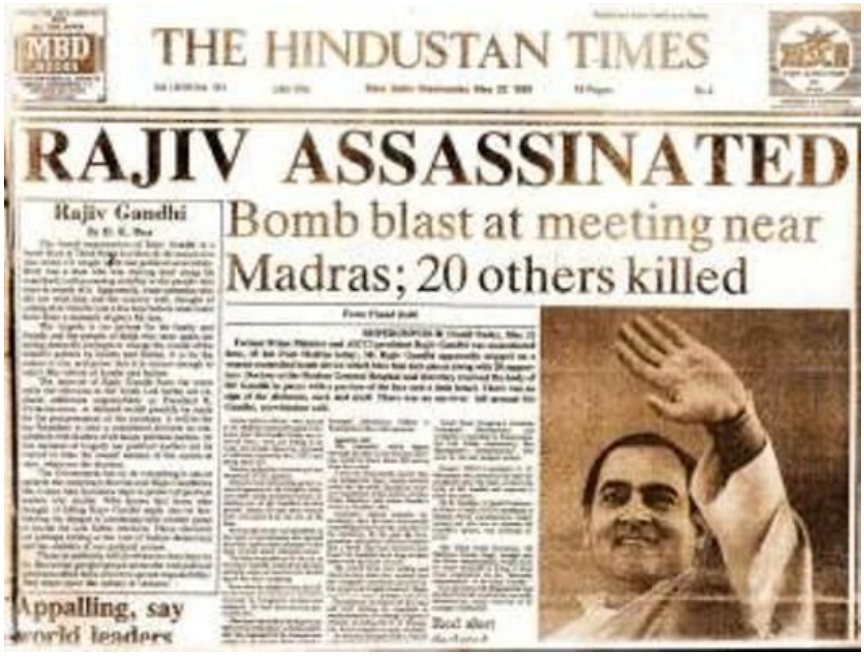

TERROR INCIDENTS IN SOUTH ASIA - 2020
India most affected after Afghanistan
Incidents
Fatalities
AFGHANISTAN
1,156
7,679
INDIA
298
589
PAKISTAN
193
506
BANGLADESH
3
3
SRI LANKA
1
1
NEPAL
1
1
TOTAL
Incidents: 1,652
Fatalities: 8,779*

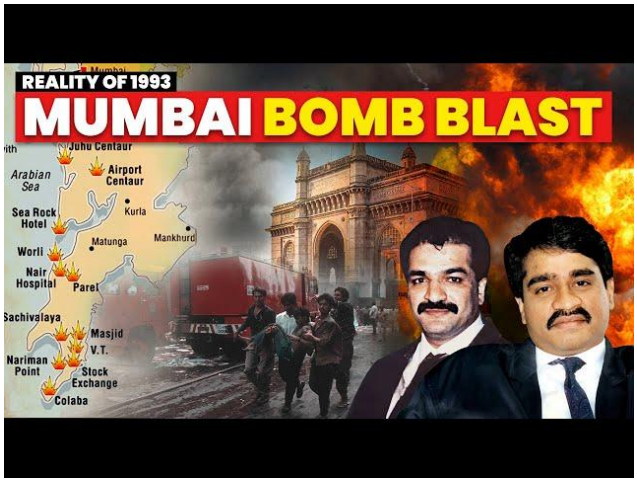

GLOBAL TERRORISM INDEX 2024
South Asian countries' scores out of 10
(Lower score indicates lower impact of terrorism)
Global rank
4th
Pakistan
7.916
6th
Afghanistan
7.825
14th
India
6.324
32nd
Bangladesh
3.317
33rd
Sri Lanka
3.072

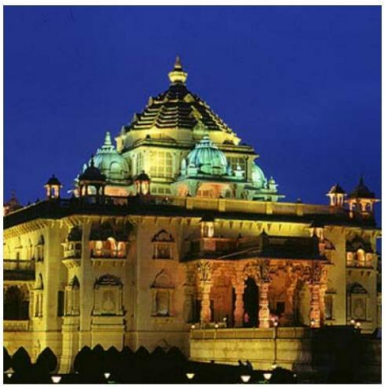
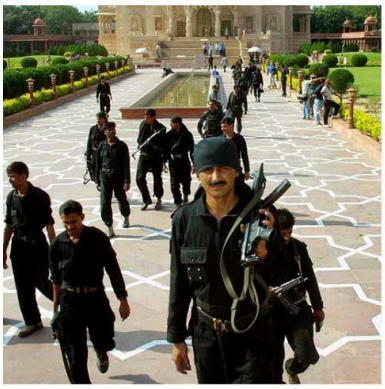

Terror-related
DEATHS in
Jammu & Kashmir
ETV BHARAT
2013
Total:172
Civilians 19
Security Forces 53
Terrorists 100
Unidentified
0 20 40 60 80 100
2014
Total:189
Civilians 28
Security Forces 47
Terrorists 114
Unidentified
0 20 40 60 80 100 120
2015
Total:175
Civilians 19
Security Forces 41
Terrorists 115
Unidentified
0 20 40 60 80 100 120
2016
Total:267
Civilians 16
Security Forces 88
Terrorists 165
Unidentified
0 50 100 150 200
2017
Total:357
Civilians 54
Security Forces 83
Terrorists 220
Unidentified
0 50 100 150 200 250
2018
Total:452
Civilians 86
Security Forces 95
Terrorists 271
Unidentified
0 50 100 150 200 250 300
2019
Total:283
Civilians 42
Security Forces 78
Terrorists 163
Unidentified
0 50 100 150 200
2019
(Till August 4)
Total:233
Civilians 23
Security Forces 74
Terrorists 136
Unidentified
0 20 40 60 80 100 120 140
2019
(From August 5)
Total:50
Civilians 19
Security Forces 4
Terrorists 27
Unidentified
0 5 10 15 20 25 30
2020
Total:321
Civilians 33
Security Forces 56
Terrorists 232
Unidentified
0 50 100 150 200 250
Source: Jammu and Kashmir Police

Mention various incidents hampering National Security of the Country?

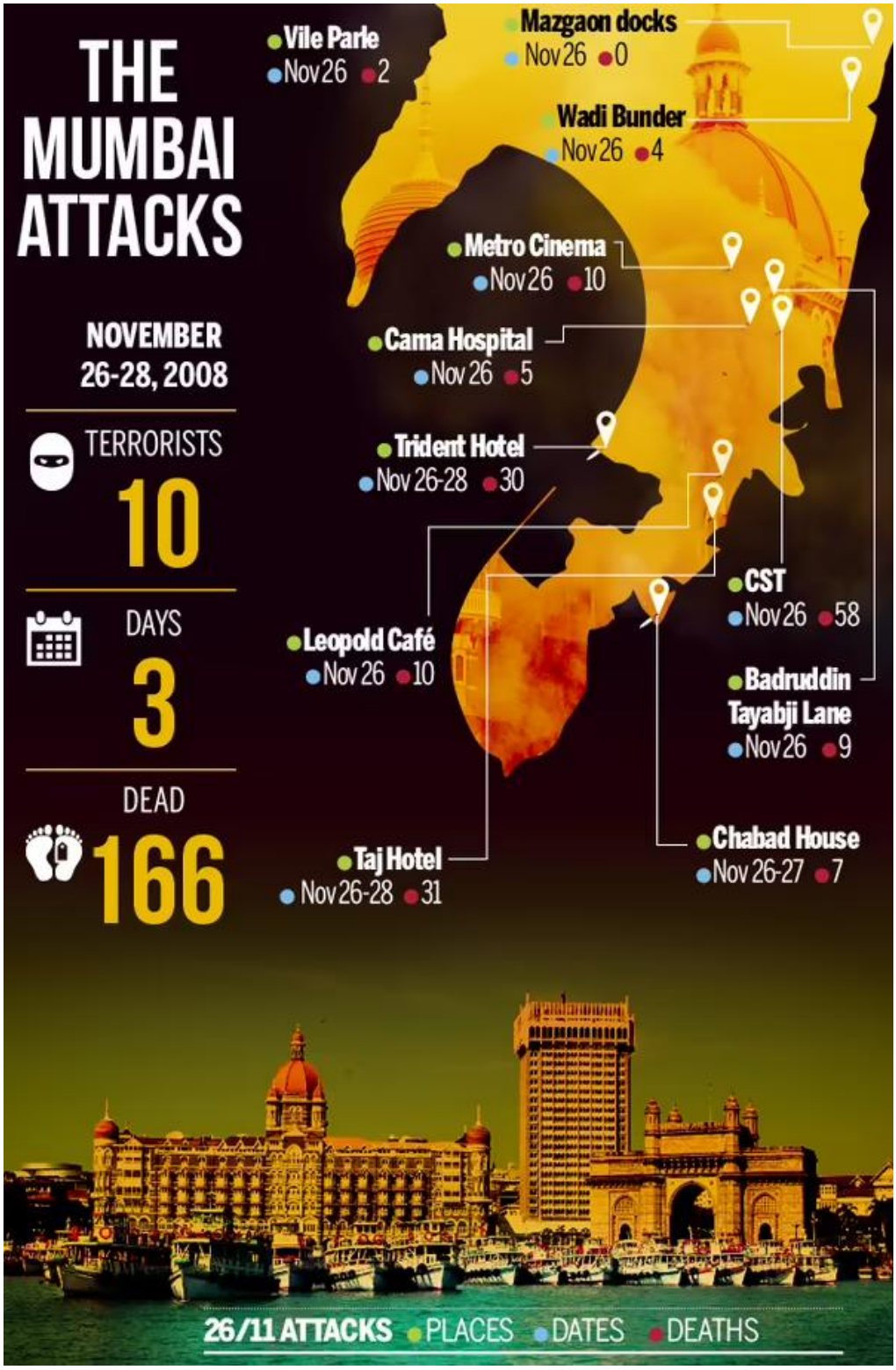


Terror incidents	Description
May 1991, Sriperumbudur	● Former **Indian Prime Minister Rajiv Gandhi** was blown up by a **suicide bomber from the Liberation Tigers of Tamil Eelam** during a campaign rally. 

March 1993, Mumbai	● In the single deadliest attack in independent India's history, **multiple bombs exploded across the city, killing more than 250 people**. ● Police blamed fugitive **Indian gangster Dawood Ibrahim** and his aides for the attack. 
2001 Indian Parliament attack	● The **2001 Indian Parliament attack** was a terrorist attack on the **Parliament of India in New Delhi, India, on 13 December 2001.** ● The attack was carried out by **five Jaish-e-Mohammed terrorists** that resulted in the **deaths of six Delhi Police personnel, two Parliament Security Service** personnel, and a **gardener.**

Akshardham Temple attack,2002	• On **24 September 2002,** multiple terrorists attacked the **Swaminarayam Akshardham complex in Gandhinagar, Gujarat**, India, **killing 33 and injuring more than 80.** • India's **National Security Guard intervened** and ended the **siege the next day, killing the terrorists.**  
July 2006, Mumbai	• **More than 200 people were killed** when a **series of bombs exploded on multiple trains** of the **suburban rail network** used by millions of people daily.

September 2006, Malegaon	● Explosions near a **mosque in Malegaon, a city in the western state of Maharashtra**, killed at least 45 people. ● Authorities blamed **Abhinav Bharat, but all the accused were later acquitted.**
May 2008, Jaipur	● More than **70 people died in nine explosions** in the **capital of India's western state of Rajasthan.** ● Authorities blamed the **Indian Mujahideen**.

November 2008, Mumbai	• More than **170 people were killed and more than 300 were injured in attacks carried out by LeT.** 

Enlist agencies involved in protecting national security?

Agencies	About
Indian Armed Forces	• The **Indian Armed Forces are the military forces of the Republic of India.** • It consists of **three professional uniformed services: the Indian Army, the Indian Navy, and the Indian Air Force.** • **Indian Army:** ○ The **land-based force, securing borders and sovereignty against land threats, the world's largest volunteer army.**

- **Indian Navy:**

  - Protects **maritime interests, sea lanes, and conducts coastal defence, with specialized units like MARCOS for special ops.**

- **Indian Air Force:**

  - Provides **air power, defence, and strategic airlift, expanding reach across oceans.**

National Investigation Agency (NIA)	**NIA is India's premier counter-terrorism law** enforcement agency, similar to the **FBI in the USA.** It **investigates and prosecutes** offenses affecting the **sovereignty, security, and integrity of India.** ● Investigate **terrorism-related cases** and offenses under Acts such as: ○ **Unlawful Activities (Prevention) Act (UAPA)** ○ **Atomic Energy Act** ○ **Anti-Hijacking Act** ○ **Weapons of Mass Destruction Act** ● **Coordinate with state police and intelligence** agencies. ● Maintain data on **terrorist activities and networks.** ● Prosecute individuals **involved in terrorism and organized crime** linked to national security.
Intelligence Bureau (IB)	The **Intelligence Bureau** is India's **domestic intelligence, counter-intelligence, and internal security** agency similar to the **FBI (USA) or MI5 (UK).** **Key Functions:** ● **Internal Security:** Collects **intelligence on threats within India — terrorism, extremism, separatism, and espionage.** ● **Counter-Intelligence:** Prevents **infiltration or spying by foreign intelligence agencies.** ● **Political Intelligence:** Monitors **potential internal political instability** or **anti-national activities.** ● **Border Security Coordination:** Works with **RAW, NIA, and paramilitary forces** to manage security along sensitive borders. ● **Security Clearances:** Conducts background checks for **government appointments and sensitive positions.**

	• **Cyber & Communication Surveillance:** Tracks **online radicalization, cyber threats, and communication intercepts (under lawful authority).**
Research and Analysis Wing (R&AW) 	**The Research & Analysis Wing (R&AW)** is the foreign **intelligence agency** of the Government of India. It is responsible for the **collection, processing and assessment of intelligence outside India's borders** deemed vital for the **advancement of the country's national security interests.** **Key Functions:** • **Foreign Intelligence Collection:** Gather information on **political, strategic, military, and economic developments** in other countries. • **Counter-Terrorism & Counter-Intelligence:**Tracks **foreign terror networks** and **prevents cross-border** threats to India. • **Strategic & Covert Operations:** Conducts **covert missions to protect India's national interests abroad.** • **Security of India's Interests Overseas:** Protects **Indian embassies, diplomats, and assets** in foreign nations. • **Nuclear Security Intelligence:** Monitors activities related to **nuclear proliferation and technology transfers.** • **Intelligence Liaison:** Maintains **cooperation with global intelligence** agencies for **mutual security.**
National Security Guard (NSG)	The **NSG** is a special forces unit under the **Ministry of Home Affairs (MHA).** It is trained for **counter-terrorism, anti-hijacking, and hostage rescue operations** — similar to S**WAT (USA) or SAS (UK).**

Key Functions:

- **Counter-Terrorism Operations:** Neutralize **terrorists, rescue hostages, and defuse explosives.**
- **Anti-Hijacking Operations:** Respond to **aircraft hijackings and similar crises.**
- **Bomb Disposal & EOD Operations: Detect and defuse bombs or IEDs.**
- **VIP Security:** Protect select **high-risk dignitaries (e.g., Prime Minister, top political leaders).**
- **Disaster Response Support:** Occasionally assists during **emergencies like explosions or terror threats.**

National Technical Research Organisation (NTRO)

NTRO is a technical intelligence agency that gathers **signals, imagery, cyber, and satellite intelligence.**

It is not a **law enforcement or field agency.**

It works mainly through **technology-based intelligence collection.**

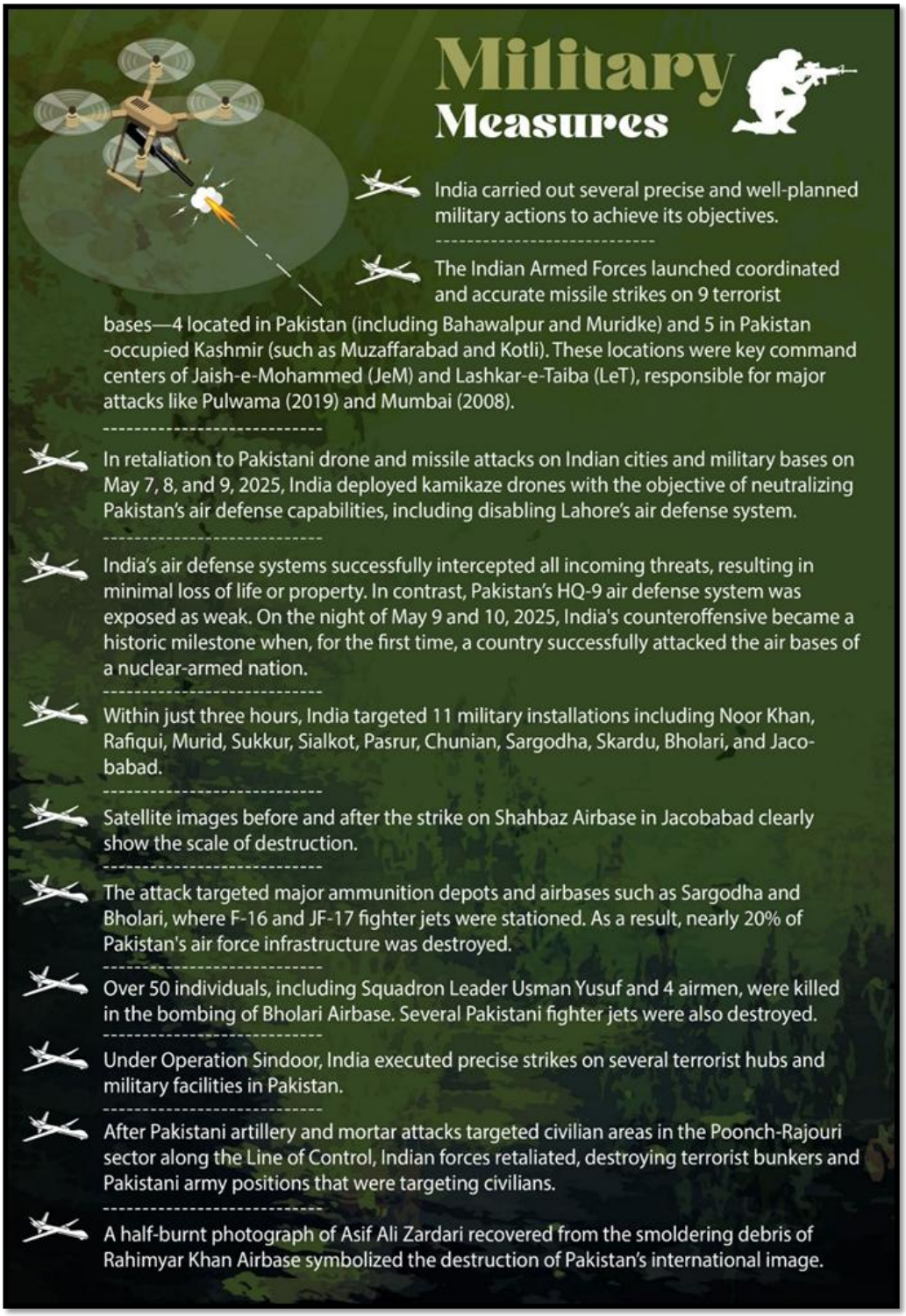
Key Functions:

- **Satellite Surveillance (IMINT):** Collects imagery **intelligence using satellites** for **defense and border monitoring.**
- **Signals Intelligence (SIGINT):** Monitors **radio, radar, communication, and electronic signals from hostile** entities.

	• **Cyber Intelligence & Security:** Tracks **cyber espionage, hacking attempts**, and **digital** warfare threats against India. • **Aerial Reconnaissance:** Uses **drones, aircraft, and satellites for strategic surveillance.** • **Technical Support to Other Agencies:** Assists **RAW, IB, DRDO, Armed Forces, and NIA with high-end tech data.** • **Infrastructure Protection:** Monitors and secures **critical information infrastructure — power grids, satellites, defense systems**, etc.
Anti-Terrorism Squads (ATS)	An **Anti-Terrorism Squad (ATS)** is an I**ndian special counterterrorism unit** present in several state police agencies of India including **Maharashtra Police, Gujarat Police, Kerala Police, Uttar Pradesh Police, Rajasthan Police, Bihar Police, Jharkhand Police,Tamil Nadu Police, Madhya Pradesh Police and Chhattisgarh Police.** These units are frequently involved in the **investigative, intelligence and emergency** response aspects related to **terrorism and cooperate** with other branches of their **police departments, police forces** from other states, and national agencies such as the **Intelligence Bureau and the National Investigation Agency.**

	Key Functions of ATS ● **Counter-Terrorism Operations: Detect, prevent, and investigate terrorist activities** within the state. ● **Intelligence Gathering:Collect information** on **terrorist sleeper cells, radical networks**, and illegal arms trade. ● **Coordination with Central Agencies:** Share **intelligence** and **support operations with NIA, IB, and NSG.** ● **Cyber Surveillance:** Track online **radicalization, fake news, and terror funding through digital means.** ● **Explosives and Bomb Disposal:** Handle cases involving I**mprovised Explosive Devices (IEDs) and bomb threats.** ● **Arms & Narcotics Control:** Bust arms **smuggling, counterfeit currency, and terror funding networks.**

Enlist various initiatives taken to protect the national security of the country?



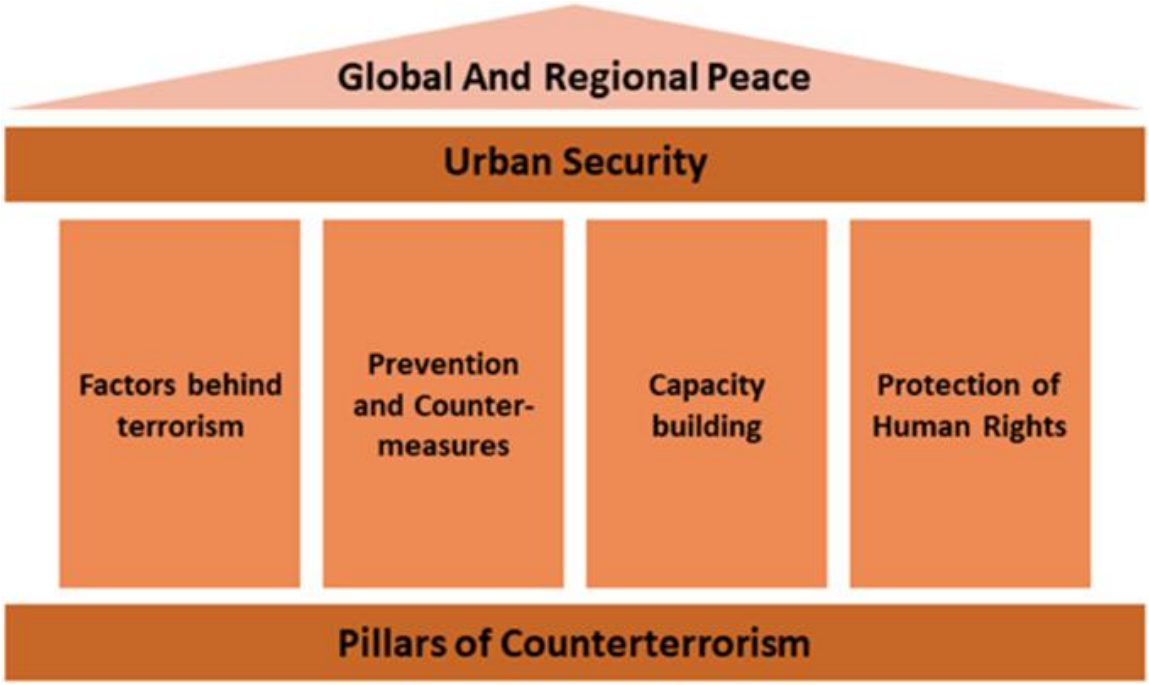
- As per the **seventh schedule** to the **Constitution of India, 'Police' and 'Public Order'** are the subjects of the **States**.

- However, to deal with the **challenges of internal and border security** and to **combat internal** as well as **cross-border terrorism,** Government of India follows a **multi- dimensional strategy, which entails various measures.**

Measures	Description
Strengthening internal & border security	• Enhancement of **counter insurgency grid.** • Deployment of **Central Armed Police Forces (CAPFs).** • Special focus on **modernization and strengthening of security equipment.** • Organizing various **capacity building programs for State Police Forces, Law Enforcement Agencies and Cyber Investigative Agencies.** • Augmenting **intelligence capabilities and strengthening law enforcement agencies** and ensuring sharing of intelligence inputs on a real-time basis, amongst **all security forces.** • Implementation of the **Comprehensive Integrated Border Management System (CIBMS), incorporating sensors, cameras, ground surveillance radars and command-control systems.** • Deployment of **Unmanned Aerial Vehicles (UAVs), Drones and Satellite Surveillance in vulnerable border areas.** • Construction of **strategic roads, tunnels and bridges** in border areas under the **Bharatmala and Border Road Organization initiatives.** • **Day & night area domination.** • **Round-the-clock Nakas** at strategic points. • Construction of **fences, floodlighting, Border Out Posts/ Company Operating Bases, building roads and Integrated Check Posts (ICPs)** at various locations on the international borders and measures to strengthen Coastal **Security.**

	● Regular **Border-Coordination meetings** and joint patrolling with neighboring countries like **Bangladesh, Nepal and Myanmar.**
Preventing internal and cross-border terrorism	● While adopting **'Zero-Tolerance' policy** against **terrorism**, following key measures have been taken - ○ **Effective, continuous and sustained actions** against terrorists and support structures. ○ Dismantling of the terror **ecosystem using the whole of government approach.** ○ **Preventive operations through Central Armed Police Forces (CAPFs), Indian Army and State Police Forces** involving identification of strategic supporters of terrorism and initiating investigations through **NIA to expose their mechanisms of aiding and abetting terrorism.** ○ Strengthening legal regime like **Unlawful Activities (Prevention) Act, 1967 and National Investigation Agency Act, 2008** for effective prosecution of terrorist organizations and individual terrorists. ○ Use of **Artificial Intelligence, Big Data Analytics and Facial Recognition Tools to detect terrorist networks** and activities. ○ **Monitoring of social media and cyberspace to prevent online radicalization.**
Stop financial support to terrorist	● A **"Combating Financing of Terrorism (CFT) Cell"** has been established in the **Ministry of Home Affairs since 2011** to coordinate with various intelligence/enforcement agencies to **prevent financing of terrorism.** ● A Terror Funding and Fake Currency Cell (TFFC) has also been established in the **National Investigation Agency (NIA)** to investigate and prosecute terrorist funding and **Fake Indian Currency Notes (FICN)** cases.

	• A **FICN Co-ordination Centre (FCORD)** is also functioning to share the **intelligence/ information amongst the different security agencies of Centre/States** to counter the circulation of Fake Indian • **Currency Notes within the Country.** • Monitoring of **suspicious financial transactions, NGOs** and **hawala channels through coordinated actions** with financial intelligence agencies.



What is the relevance of the topic for UPSC CSE?

- **Prelims:** Organized crime, insurgency in India's northeastern states, National Investigation Agency, National Security Guard, Unlawful Activities (Prevention) Act (UAPA), 1967, National Security Act (NSA), 1980.
- **Mains:** Issues Related to Terrorism in India, Internal Security Architecture in India.

SOME PREVIOUS YEARS PRELIMS QUESTIONS.

Q.1 Consider the following statements: (2023)

1. According to the Constitution of India, the Central Government has a duty to protect States from internal disturbances.
2. The Constitution of India exempts the States from providing legal counsel to a person being held for preventive detention.?
3. According to the Prevention of Terrorism Act, 2002, confession of the accused before the police cannot be used as evidence.

How many of the above statements are correct?

(a) Only one

(b) Only two

(c) All three

(d) None

Ans. (b)

SOME PREVIOUS YEARS MAINS QUESTIONS

Q.1 Terrorism is a global scourge. How has it manifested in India? Elaborate with contemporary examples. What are the counter measures adopted by the State? Explain. **(2025-10 Marks)**

Q.2 Explain how narco-terrorism has emerged as a serious threat across the country. Suggest suitable measures to counter narco-terrorism. **(2024-10 Marks)**

Some questions from this year and previous years interview transcripts.

Board Sanjay Verma sir:

- How to deal with pakistan on terrorism?

Board Sanjay Verma sir:

- What is nuclear deterrence ?
- Does nuclear deterrence work only for other NWS or non NWS also?
- What is extended deterrence?
- Has nuclear deterrence worked in the case of India - Pakistan ?

Board Sheel Vardhan sir:

- Tell me the difference between insurgency and terrorism?
- What is naxalism- insurgency or terrorism?

Board Sheel Vardhan Singh sir:

- What is economic terrorism?
- How can India counter this economic terrorism?

Board BB Swain sir:

- What is Narco Terrorism?
- What are various internal security problems of India?

Board Dinesh Dasa sir:

- What is legal terrorism? Can you give any example ?

Some questions for QUIZ.

Q.1 Consider the following statements regarding NATGRID.

1. The National Intelligence Grid (NATGRID) functions under the Ministry of Home Affairs
2. The headquarters of NATGRID is located in Bengaluru
3. NATGRID was conceptualized after 2001 Parliament Attack.

How many of the above statements is/are correct?

(a) Only one

(b) Only two

(c) All three

(d) None

Ans. (a)

Some questions for POLL.

Q.1 Do covert operations differ from conventional military operations in terms of deniability?

(a) YES

(b) NO

(c) Can't say.

Q.2 Can covert operations raise ethical and legal concerns under international law?

(a) YES

(b) NO

(c) Can’t say.

Q.3 Do democratic states conduct covert operations despite transparency norms?

(a) YES

(b) NO

(c) Can’t say.

Q.4 Are covert operations conducted without public acknowledgment by the state?

(a) YES

(b) NO

(c) Can’t say.

Q.5 Are intelligence agencies the primary executors of covert operations?

(a) YES

(b) NO

(c) Can’t say.

Q.6 Are covert operations explicitly mentioned in India’s public national security documents?

(a) YES

(b) NO

(c) Can’t say.

Q.7 Can covert operations be used as a tool of strategic signalling?

(a) YES

(b) NO

(c) Can’t say.

Q.8 Can covert operations include cyber and information warfare?

(a) YES

(b) NO

(c) Can’t say.

■■■■