

2025 Y6 GP: Power (Part 2)

*How Power has evolved today (Technology reshaping Power),
Implications on Stakeholders and the Shift in Power Dynamics,
Uncertain Balance of Power → Need for Regulation, Control and Responsibility (next Thematic Lens)*

Recap: Part 1's Lecture on Power covered the following:

- Why consider Power
- What is Power
- Origins/Sources of power
- Who wields Power (Stakeholders)
- Manifestations/Examples of Power

Organisation of Notes – Part 2's Lecture on Power will explore the following Essential Questions (EQs):

1) How has Power evolved today?

- A. How are technological advancements **changing the nature** of power and **how it is applied**?

2) How is the Changing Nature of Power affecting Stakeholders and the Power Dynamics?

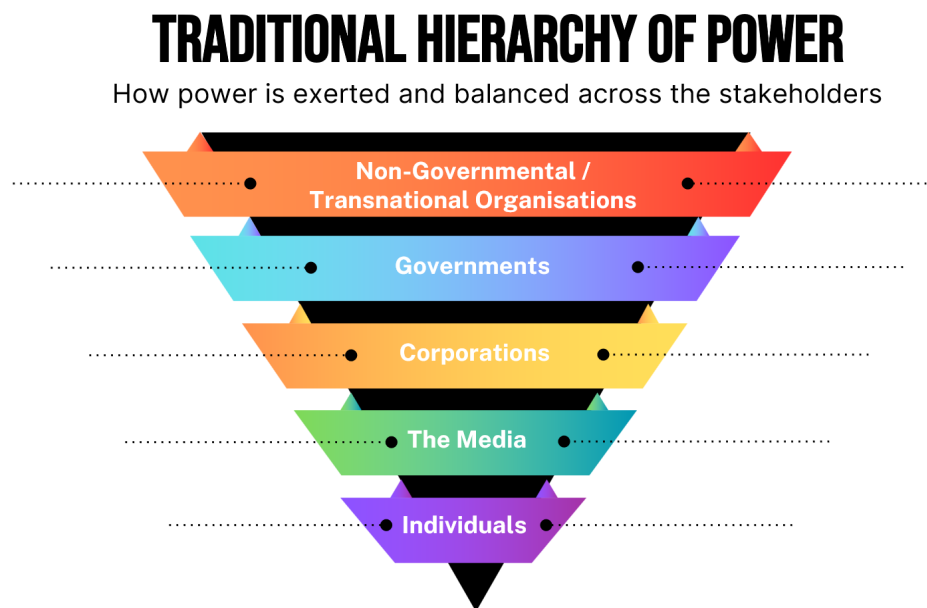
- A. How is **technology challenging** the degree of power that is traditionally held by the **government**?
- B. How is **technology strengthening** the degree of power held by **governments** today?
- C. How is **technology shaping** the degree of power that **individuals** have today?

Significance of these Essential Questions (EQs):

- ★ 1: **Conceptual Understanding** - Examining how power **changes across time**.
- ★ 2: **Conceptual Understanding** - Examining the **power relationships across stakeholders** - technology shaping the degree of power that governments and individuals have - under different political systems **across different societal contexts**.

1. How has Power evolved today?

Traditionally, power used to be exerted from a top-down, unidirectional manner. Non-governmental organisations held governments accountable, and governments had direct control over corporations and individuals. The conventional view of how power is exerted across the stakeholders looks like this:



However, today, as technology leapfrogs and pushes the frontiers of knowledge, its practical solutions have solidified our trust in it. Our *increasing reliance on technology and its ubiquity is profoundly reshaping the balance of power* between governments, corporations, the media, and individuals.

Today, Big Tech companies are emerging as a powerful entity that possess:

Hard power in the form of:

- 1) **Resources / Wealth:** Economic power — control over material resources, money, or capital that is at times larger than what governments possess.
- 2) **Knowledge / Expertise:** Intellectual or technical power — having information or specialised skills other stakeholders lack or depend on technology to guide decision making and actions.

Soft power established through:

- 3) **Networks / Relationships:** Power through forming alliances, connections, and collective support with other research agencies and tech companies.
- 4) **Legitimacy / Recognition:** Power granted by collective belief in and reliance on science-based, research-backed, data-driven analyses and solutions.

A) How Are Technological Advancements Changing Power?

1. **Rise of Big Tech** – Companies like Google, Meta, and Amazon control vast amounts of data, influencing behaviour, elections, and even national security.
2. **Cyber Warfare and Hacking** – Countries now use cyber-attacks to gain power over others (e.g., Russian interference in U.S. elections).
3. **Decentralised Finance (Cryptocurrency)** – Weakening traditional banks' and governments' hold on money.

As a result of the rising power of technology and Big Tech companies, *some have argued that states which traditionally held dominant control, are now seeing the absolute terms of their power being undermined*. State power is viewed as *increasingly decentralised and redistributed by Big Tech companies*, who have succeeded, in some cases, in weakening governments' authority over their people. From this perspective, *digital platforms, AI, and big data* are said to have arguably upended the power hierarchy, increasingly *having the means to advance corporate agendas and empower individual civilians* to the detriment of weakened political control.



How is this evolving nature of power shaping the issues we debate about in GP?

Let's take a look at some past year A level questions that examine and evaluate the evolving relationships of power between two stakeholders:

1. 'Power these days lies more with the people than the politicians.' To what extent is this true? (2021)
2. Is modern technology a **benefit or threat** to democracy? (2020)
3. Consider the view that social media has **more influence than politicians**. (2019)

Common across these questions is the *changing context of how power is acquired and applied (Conceptual Understanding)* across these stakeholders. It is necessary to **consider how technology has influenced the degree of power** that each of the stakeholders have.

The following section will explore how technology both **empowers** and **disempowers** the government (of different political systems), corporations, and individual civilians.

2A) Technology and Government: How governmental power today is **challenged** by technology

Tech companies are increasingly undermining government power in multiple ways. Their influence extends across the regulation of information flows, challenging the digital sovereignty of governments, and interfering with their ability to do law enforcement. Here are some ways in which tech giants are eroding traditional state control:

1. Controlling the Digital Public Sphere: Influencing political discourse, curbing information flows

Tech companies now **moderate political discourse** and **control what information reaches** the public, sometimes against government interests.

A) Social media platforms can weaken political authority

- Private tech platforms are now setting the rules of engagement, including content moderation and algorithmic gatekeeping or prioritisation of information.
- Tech companies like Meta (Facebook), Twitter (X), and Google control digital spaces where political discourse occurs. As platforms for civic engagement, social media algorithms influence what the public reads and how public opinion unfolds. This directly shapes the outcomes of voters' participation in elections, which determine the political longevity of governments.

B) Censorship of politicians and facilitating organised civil protests

- Digital platforms can now de-platform politicians and subvert the traditional power dynamic that assumes only the government has the power to censor and exert control.
- In authoritarian states, platforms like TikTok and YouTube have become battlegrounds where governments try to exert censorship, but are increasingly met by activists who use them to organise resistance. These social media platforms have allowed civilians to bypass state censorship to facilitate organised movements that topple the ruling dictatorships in some countries - e.g., Facebook and Twitter's role in the Arab Spring.

Example - Relevant details that demonstrate how technology counteracts politicians' authority	Significance of the Example - What does it show about how governmental power is curtailed/limited by technology?
 Example 1: Twitter and Facebook Banning Donald Trump (2021) - After the January 6 Capitol riots, Twitter and Facebook permanently suspended Donald Trump's accounts, citing the risk of inciting violence. - The US government did not order this. Instead, private companies unilaterally silenced a sitting president, demonstrating control over political speech.	<i>Tech companies can censor and de-platform politicians, limiting their digital outreach and influence over the masses.</i>

 Example 2: YouTube's role in sabotaging Russian propaganda efforts to justify the Russia-Ukraine War to its citizens • YouTube removed Russian state-backed media (RT and Sputnik) from its platform globally, affecting Russia's ability to spread its narrative about the war. • This action bypassed government censorship and propaganda controls, challenging Russia's information dominance.	<i>Tech companies can dispel political propaganda and curtail government power by blocking such content from reaching its people.</i>
---	--

2. Challenging governments' ability to perform key duties (e.g. surveillance for national security and law enforcement)

Tech firms now **control access to data** and can wilfully **resist government demands** for surveillance.

A) End-to-End Encryption: Difficulty to bypass to carry out security checks

- Apps like WhatsApp and Telegram provide encrypted communication, shielding users from government surveillance and making it harder for law enforcement to track criminals or dissenters.
- Despite governmental pressure worldwide on tech firms to create backdoors in encryption, companies like Apple have resisted requests from countries like the US and China.

B) Conflicting claims to the right to access data

- Tech firms like Apple and Google have also refused to unlock devices for law enforcement, citing user privacy rights.
- Amazon's Ring and facial recognition technology raise concerns about surveillance powers shifting from governments to private corporations.

Example - Relevant details that demonstrate how technology counteracts politicians' authority	Significance of the Example - What does it show about how governmental power is curtailed/limited by technology?
 Example 1: WhatsApp Refusing to Create Encryption Backdoors (2019-2022) • Governments (US, UK, Australia) pressured WhatsApp to weaken end-to-end encryption to help law enforcement access messages. • WhatsApp refused, prioritising user privacy over government demands, leading to tensions with security agencies.	<i>While surveillance technology has earned a bad rep for its usage by some authoritarian governments to monitor and control their citizens, <u>in cases where national security is at potential jeopardy, big tech companies can now directly intercept and curtail government efforts to do background security checks on high-risk individuals</u>. This is a <u>major setback to the</u></i>

 Example 2: Apple vs. FBI – iPhone Encryption Battle (2016, 2020) • The FBI demanded Apple unlock the iPhone of a terrorist involved in the San Bernardino shooting. • Apple refused, arguing it would create a dangerous precedent for user privacy. • The FBI had to hire private hackers, showing that governments no longer have full control over digital security.	<i>government's efficacy to ensure the safety of the country and its people.</i>
---	---

3. Difficulty containing Big Tech companies' expanding geopolitical influence

A) **Digital sovereignty battles: Big Tech vs. National governments**

- **Digital sovereignty** refers to a country's ability to protect and control its digital assets, including data, infrastructure, and networks. It is one of the most pressing issues in the regulatory landscape.
- **For governments**, it entails having **the ability to govern the internet within their country's borders**, safeguard their citizens' privacy, and secure the country's critical infrastructure.
- With **64.4 percent** of the total population being online, **digital sovereignty is a priority today** for governments worldwide. **But achieving it is not a straightforward task** due to the following reasons:

- ★ **Digital platforms increasingly challenge state sovereignty** – Social media and cloud providers dictate access to information.
- ★ **Big tech's infrastructure control gives leverage** – Internet providers (like Elon Musk's Starlink) can override government censorship.
- ★ **Tech companies can evade or delay compliance** – Using legal battles, threats, and workarounds.

Example - Relevant details that demonstrate how technology counteracts politicians' authority	Significance of the Example - What does it show about how governmental power is curtailed/limited by technology?
 Example: The U.S. vs. TikTok (2020-Present) – National Security vs. Corporate Resistance • TikTok (owned by China's ByteDance) was labelled a national security risk by the Trump administration due to concerns over data access by the Chinese government. • Trump signed an executive order attempting to force TikTok's sale to a US company (Microsoft/Oracle).	<i>The US vs. TikTok battle is an example where a government (US) perceives a foreign-owned platform as a national security threat. A foreign-owned tech company defied the executive order of a U.S. president, delaying regulatory action for years while continuing operations. This shows how governments today have to jostle for control and have their power overridden by tech giants on matters directly related to national sovereignty.</i>

- TikTok resisted, sued the US government, and won temporary court rulings delaying the ban.
- Biden's administration continued the security review, but TikTok remains operational in the US, demonstrating its ability to resist state intervention.

*While technology poses significant challenges to absolute government control in some countries, in other contexts, it has been an **enabling factor** that **entrenches** government power, sometimes to the detriment of the people.*

2B) Technology and Government: How technology **strengthens** governments' power and increases the **potential for abuse and misuse**

In authoritarian states, technology enhances government power through **surveillance and censorship**.

1. Power Over Individuals: The Surveillance State

Mass Surveillance and AI Policing: More governments are leveraging technology to exert unprecedented control over individuals, monitoring citizens and predicting dissent.

How this can descend into abuse and misuse:

- ★ **Suppression of dissent:** Governments can silence critics by tracking activists, journalists, and political opponents.
- ★ **Invasion of privacy and infringement of human rights:** Mass surveillance erodes civil liberties and individual freedoms. Even democracies use surveillance technologies in law enforcement and intelligence. (e.g., TraceTogether app in Singapore as a contact tracing measure to curb the spread of the Covid-19 pandemic)

Examples:

- China's Social Credit System: Uses facial recognition AI and big data tracking to reward or punish citizens based on behaviour (e.g., limiting travel for those with "low" scores).
- China's Surveillance of the Uyghurs in Xinjiang: AI predicts potential "terrorists" (mainly targeting Uyghur Muslims), leading to mass detentions.
- NSA Mass Surveillance (USA): Leaked by Edward Snowden, revealing how the US government secretly collected data on millions of people.
- Hong Kong Protests (2019): Authorities used CCTV and facial recognition to identify and arrest protestors.

2. Controlling Access to Information and Resources:

A) Internet Censorship and Information Control: Governments use technology to control narratives and limit public access to information. The ability to block, filter, or manipulate digital content allows authoritarian regimes to maintain control.

 **How this can descend into abuse and misuse:**

- ★ **Silencing opposition:** Restricting access to independent media and opposition voices.
- ★ **Manipulating public perception:** Spreading government-approved propaganda while suppressing alternative viewpoints.

B) Cyber Warfare and Digital Propaganda: Governments use cyber tools to attack foreign states, manipulate elections, and control public opinion. AI-powered disinformation campaigns spread propaganda and fake news.

 **How this can descend into abuse and misuse:**

- ★ **Destabilising democratic processes:** Hacking elections and spreading misinformation to influence public perception.
- ★ **Harming foreign adversaries:** Cyberattacks can disrupt infrastructure, finance, and military operations.

Examples:

- The Great Firewall of China: Censors Western social media (Facebook, Google, Twitter) to maintain state-controlled narratives.
- Russia's Control of Media (Ukraine War): Russian government restricts access to Western news outlets and spreads misinformation about the war.
- 2016 U.S. Presidential Election: Russian hackers and troll farms spread disinformation and targeted voters to manipulate the outcomes of the election via social media.
- Cambridge Analytica Scandal: Misuse of Facebook data to manipulate political campaigns.

C) Controlling Digital Currency and Financial Transactions: Governments are pushing for central bank digital currencies (CBDCs) to monitor and control transactions. Cryptocurrency regulations allow authorities to freeze assets and prevent dissenters from accessing funds.

 **How this can descend into abuse and misuse:**

- ★ **Financial repression:** Blocking accounts of political opponents or activists.
- ★ **Tracking every transaction:** Eliminating financial privacy.

Examples:

- Canada's Freezing of Protestors' Bank Accounts (2022): During the Trucker Protests, the government froze bank accounts of individuals funding the movement.
- China's Digital Yuan: Allows full government control over citizens' spending.

3) Technology and Individual Power: How technology *strengthens* individuals' power to stand up against abuse or misuse of power

In **democracies**, technology both *empowers* individuals (through activism and free speech) and weakens government authority (through enabling corporate monopolies and introducing the challenge of managing the effects of misinformation on political legitimacy).

Technology *Empowers* Individuals in Overriding State Control:

A) VPNs and Circumventing Censorship

- ★ Virtual Private Networks (VPNs) help individuals bypass government-imposed internet restrictions.
- ★ Used to access blocked websites, news, and social media in authoritarian states.

👉 Examples:

- China's Great Firewall – Citizens use VPNs to access Google, Facebook, and foreign news sites.
- Russia's War Censorship (2022) – Russians used VPNs to access independent news about the Ukraine war.
- Iran Protests (2022) – VPNs allowed Iranians to bypass social media bans and organise demonstrations.

B) Blockchain and Decentralised Information Storage (Tor, Signal, Bitcoin)

- ★ Blockchain technology ensures tamper-proof documentation of human rights abuses and government crimes.
- ★ Data cannot be erased or altered by oppressive governments.

👉 Examples:

- Uyghur Human Rights Violations (China) – Blockchain-based records prevent China from erasing evidence of Uyghur persecution.
- Hong Kong Protests – Protesters used blockchain to store protest information after China censored online records.

C) Online Petition Platforms and Digital Advocacy and Resistance

- ★ Websites like Change.org, Avaaz, and MoveOn allow individuals to rally support for causes.
- ★ Governments are pressured by mass online petitions and digital campaigns.

👉 Examples:

- Save the Internet Campaign (India, 2016) – Over 1 million people signed an online petition that forced the government to protect net neutrality.
- Rohingya Crisis Petition (2017) – Global petitions pressured Myanmar to address human rights abuses.

Summary and Conclusions

Modern Context: The Evolving Nature of Power

- ★ Power is **shifting rapidly** in the modern world due to technology.
- ★ Globally, **tech giants/corporations** *increasingly rival states in power, as their platforms shape public opinion, economies, and even political outcomes.*
- ★ The central question is **whether governments can adapt fast enough to regulate and balance power in a rapidly digitising world** — or whether power will continue shifting toward private entities and decentralised networks.
- ★ While **governments still hold military and legal power**, *tech firms now control key aspects of finance, communication, surveillance, and information flow.*
- **In democracies**, tech companies **challenge** traditional state roles but still face regulation attempts (antitrust cases, data privacy laws).
- **In authoritarian regimes**, some governments **co-opt** technology to strengthen control (China's AI surveillance, Russia's internet restrictions).
- The battle between **state control vs. corporate power** is ongoing, but **Big Tech is increasingly behaving like sovereign entities**, shaping the world's political and economic future.

Changing Nature of Power and its Implications on Stakeholders

- ★ **Governments** are both **given more tools to exert control**, while also **simultaneously challenged** by technology in having absolute power and control over their people and protecting national sovereignty.
- ★ While technology **empowers individuals**, it can also be **disempowering** as it enables new forms of control and abuse by the government, jeopardising fundamental human rights to freedom of access to information, expression and assembly, to name a few.

The Future Ahead: What Now?

- ★ The evolving nature of power thus calls for the **need for checks and balances**: While technology enhances government efficiency, it also amplifies the risk of authoritarian control, surveillance, and abuse. The challenge is to balance national security with individual rights and implement strong legal frameworks to **prevent misuse**.
- ★ The key challenge lies in **finding a balance between power, control and responsibility**.

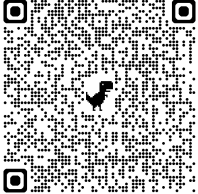
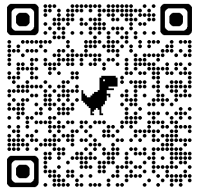
Seminar: Reading of Case Studies and Discussion Questions

- Do you think governments can reassert control over tech, or **are we moving toward a world where corporations are more powerful than nations?** Who do you think ultimately wins in the tech-government power struggle? Are we / Will we be seeing a **shift from state power to tech oligarchies?**
- **Should governments have unrestricted access to technology** *for national security*, or should there be strict regulations?
- **Should governments have more control over technology** *to prevent its misuse*, or would this limit freedom?

Application: Is modern technology a benefit or threat to democracy? (GCE 2020)

For Seminar Use: Case studies

How governments *abuse* the affordances of technology *to consolidate their power*

Philippines: The Duterte administration (2016-2022) propagated securitised narratives (such as the war on drugs and the threat of communist insurgency) to justify draconian policies, including extrajudicial killings and arrests of government critics. These narratives were reinforced through online disinformation campaigns mostly spewed by organised 'troll' farms. The government has also been accused of employing disinformation campaigns and online harassment to target journalists and dissenters. The Cybercrime Prevention Act also raised concerns about potential overreach in regulating online expression.	
<u>Thailand: Cyber Crime Act Tightens Internet Control</u> Sweeping Powers to Censor, Stifle Free Speech, Silence Critics The Thai government has implemented extensive internet censorship and surveillance, particularly focusing on content deemed critical of the monarchy. Laws such as the Computer Crime Act have been used to prosecute individuals for online activities, leading to increased self-censorship among netizens.	
<u>Deluge of Digital Repression Threatens African Security</u> Concerning trend of politically motivated internet shutdowns: African governments are using the pretext of security to restrict digital communications and citizens' rights. In the process, they are inadvertently contributing to economic losses and greater instability. One notable example is Ethiopia. The Ethiopian government has employed internet shutdowns and surveillance to control information flow and monitor opposition activities. These measures have been used to suppress dissent and limit the organisational capabilities of opposition groups.	