ISC

STUDY GUIDE

2025

COLOMBO MODEL UNITED NATIONS

Intelligence Sharing Coalition

Agenda

Practice Debate 1: The Importance of Cross-Border Intelligence Sharing in Strengthening Counter-Terrorism Efforts.

Practice Debate 2: Reforming Intelligence Agencies to Maintain Ethical Practices with emphasis on Politicization.

Conference: The Consequential Influence of Intelligence Agencies on Modern Conflicts

Message from the Chairs

The Intelligence Sharing Coalition is dedicated to encouraging vigorous debate and discussion regarding the know-how of intelligence operations of each state. The ISC would give immense opportunity to representatives to not only question and be highly critical of various operations by geopolitically opposing nations, but to also reshape and amend current cross-border intelligence-sharing communities (like the Five-Eyes community between much of the Western world). Furthermore, our vision of the ISC is one in which delegates can draw parallels between intelligence operations of the past and pressing conflicts of the status quo, to identify and evaluate the role of the agencies within the ISC in maintaining global peace and security.

Given the complexities of most nations' intelligence sectors, we hope this study guide can clue you in on understanding the nuanced role of each faction within each intelligence agency as these perspectives are crucial in bringing both diversity and clarity to debate. It is extremely unorthodox to have opposing intelligence agencies sit down together around a table, and discuss pertinent issues relating to both national and international security. It is this unorthodox confrontation, between say the US's NSA and Russia's FSB - that would lead to critical debate regarding each other's operations and policy plans. On a final note, we wish that delegates understand that global intelligence agencies require both regulation and advancement to deal with emerging threats to global security and that this development can only be achieved through cooperation.

We hope to see intense and constructive debate - see you at the conference!

- *Nadeem and Sanchitha*

Mandate

The ISC's mandate would be universal just like that of a traditional Security Council. Nevertheless, this study guide magnifies on pertinent issues ranging from intelligence matters like foreign espionage, active threats to counterterrorism efforts, cybersecurity, and warfare. Delegates are allowed to branch out from the study guide and bring in diverse points of contention to foster fruitful debate. Furthermore, we would like to clarify that we expect delegates to highlight and draw links to; the exclusive edge provided by intelligence sharing in maintaining this security, as well as the necessity of ensuring that the coalition’s agencies opt for ethical, just and effective practices when carrying out their operations.

A crucial differentiator between the ISC and a traditional Security Council is the existence of a coalition-wide Non-Disclosure Agreement (NDA) to maintain the utmost level of confidentiality by ensuring that what is discussed at the ISC remains within the ISC; meaning that leaking of such confidential information to branches of governance outside the required level of clearance or usage of such information to track hostile actions against certain nations would face immediate international repercussions. We hope this opens the floor for the exchange of operation details and military strategies adopted by each country in the past to focus such tactics on common goals such as counterterrorism to fight back against historic incapabilities in eliminating terrorist organizations at their grassroots levels.

Furthermore, the ISC notes that intelligence agencies act as superior factions within most militaries and hence have a realm of understanding and depth of information far exceeding the sentiments readily published by the foreign ministries and politicians of these nations. This means that delegates/representatives of the ISC will be able to bring details of covert operations that members of the coalition were previously unaware of. Given that this is an inherently complex section of procedure as it involves policy shifting, we have decided to clarify how exactly we envision the committee adopting it.

1. “Policy Shifts” of significant importance must be outlined within the delegate’s Foreign Policy Statement (FPS), citing the widely-known or status quo version of the nation’s policy on that matter followed by a detailed description of what the shift is and how exactly it comes into play. This should ideally be followed up by what impact it has on the agenda at hand. These shifts should be deemed “important” and worthy of inclusion into your FPS if it is integral to current issues outlined in the agenda or study guide.
2. Every policy shift must be given justification regardless of its stature, even those within your FPS, which should follow a format of: Why current initiatives/foreign policies of your nation would make such a shift likely as well as why current or past issues deemed it such that the agency decided to take such covert actions in the first place.
3. Justifications done during comm will be considered procedurally as a statement that can only be requested once the floor is open. If the head table deems this policy to be within justification, we expect other delegates to respect its validity while at the same time maintaining their right to question the ethics/legality surrounding the nature of these revealed operations. If the head table has not deemed it as part of the nation’s foreign policy yet, then other delegates would be given the floor to challenge the validity or likelihood of such a shift/event happening in the first place.
4. Finally, please note that these policy shifts are not meant to be heinous violations of your nation’s established foreign policy nor is it to be established based on conspiracy theories but rather the revealing of covert directives within various conflict zones or over the digital landscape that have been previously denied by or waived off by these agencies as “allegations”. Moreover, it could also look like access to hidden technologies (that are within the realms of realistic possibility) which could prove pivotal in countering entities such as terrorist organizations.

We note that these policy shifts will prove useful in adding flair to the ISC by sparking innovative solutions but we urge delegates to treat it as a tool and to refrain from getting carried away as the primary focus of this committee should be productive discourse on real-world problems solvable through intelligence sharing.

Agencies

Below is the agency matrix for all intelligence agencies that will operate within the ISC. Brief introductions regarding the agency will also be provided, but do ensure that extensive additional research is also done. Note that some delegates will be representing countries with an "observer" status.

United States	Central Intelligence Agency	The CIA is the primary foreign intelligence agency of the United States, tasked with gathering, analyzing, and conducting covert operations to safeguard national security. It operates under the authority of the Director of National Intelligence, focusing on counter-terrorism, cyber threats, and geopolitical intelligence.
	National Security Agency	The NSA specializes in signals intelligence (SIGINT) and information security, providing the U.S. government with critical data on foreign communications and cyber threats. Its mandate includes safeguarding national communication systems and conducting surveillance to support national defence objectives
Russia	Federal Security Service of the Russian Federation	The FSB is Russia's principal domestic intelligence and counterintelligence agency, responsible for combating terrorism, organized crime, and foreign espionage within the country. It is a successor to the Soviet-era KGB, focusing primarily on internal security and border control.

	Main Intelligence Directorate	The GRU is Russia’s military intelligence agency, tasked with gathering strategic and operational intelligence, conducting special operations, and ensuring battlefield readiness. It plays a significant role in cyber warfare, counterintelligence, and espionage on a global scale.
United Kingdom	Military Intelligence Section 6	MI6, officially known as the Secret Intelligence Service (SIS), is the United Kingdom’s foreign intelligence agency responsible for gathering intelligence and conducting covert operations abroad. It supports national security by countering terrorism, cyber threats, and espionage.
	Government Communications Headquarters	GCHQ is the UK’s signals intelligence (SIGINT) and cybersecurity agency, specializing in intercepting and analyzing foreign communications to protect against cyber threats and support military operations. It also collaborates with allied nations in counter-terrorism and cyber defence.
China	Ministry of State Security	The MSS is China’s primary intelligence and security agency, focusing on counterintelligence, foreign intelligence, and political security. It operates extensively in cyber espionage and monitoring both domestic dissidents and foreign threats.

France	Directorate-General for External Security	The DGSE is France’s external intelligence agency, tasked with gathering foreign intelligence, countering terrorism, and conducting covert operations abroad. It plays a critical role in supporting France’s national defence and diplomatic policies.
Germany	Bundesnachrichtendienst	The BND is Germany’s foreign intelligence agency, responsible for collecting and analyzing information to protect Germany’s national security and interests abroad. It focuses on counter-terrorism, cyber threats, and economic and political intelligence.
Australia	Australian Secret Intelligence Service	ASIS is Australia’s foreign intelligence agency, tasked with gathering intelligence overseas to support national security and economic well-being. It conducts covert operations and collaborates closely with allied intelligence networks.

New Zealand	New Zealand Security Intelligence Service	The NZSIS is New Zealand's primary intelligence and counterintelligence agency, focusing on identifying and mitigating threats from espionage, terrorism, and subversion. It also advises the government on national security and supports law enforcement.
Canada	Canadian Security Intelligence Service	CSIS is Canada's principal national intelligence agency, tasked with identifying and mitigating threats from terrorism, espionage, and cyber warfare. It works both domestically and internationally to safeguard Canada's national interests.
Israel	Mossad	Mossad is Israel's foreign intelligence agency, renowned for its focus on counter-terrorism, intelligence gathering, and covert operations abroad. It is one of the most prominent intelligence agencies in the Middle East, supporting Israel's security and diplomatic objectives.

Pakistan	Inter-Services Intelligence	The ISI is Pakistan’s premier intelligence agency, tasked with gathering intelligence, conducting covert operations, and supporting Pakistan’s military and national security interests. It has played a significant role in regional geopolitics, particularly in South Asia and the Middle East.
India	Research and Analysis Wing	RAW is India’s foreign intelligence agency, responsible for gathering intelligence and conducting covert operations to safeguard India’s national security and interests abroad. It focuses on counter-terrorism, regional geopolitics, and countering espionage.
Iran	Ministry of Intelligence	The MOIS, also known as Ettela’at, is Iran’s primary intelligence and security agency, tasked with counter-intelligence, foreign intelligence, and counter-terrorism. It plays a key role in both domestic surveillance and international operations to protect Iran’s interests.

Japan	Public Security Intelligence Agency	The PSIA is Japan’s primary intelligence and counter-intelligence agency, focusing on countering domestic subversion, espionage, and terrorism. It operates primarily within Japan, supporting national security and public order.

Venezuela		
Sierra Leone		
Libya		

PRACTICE DEBATE 1: The Importance of Cross-Border Intelligence Sharing in Strengthening Counter-Terrorism Efforts

Background and Context

In an increasingly interconnected world, terrorism has evolved into a transnational threat that transcends borders, exploiting the very systems that were designed to enhance global connectivity. The globalization of communication, financial systems, and transport networks has enabled terrorist organizations to operate with unprecedented efficiency, leveraging sophisticated technologies and decentralized structures to recruit, fund and execute operations across multiple jurisdictions. These dynamics underscore the urgent need for robust cross-border intelligence sharing as a cornerstone of counter-terrorism efforts - especially with the advent of Islamist extremists and other political extremists on the far right and far left.

Effective intelligence sharing fosters collaboration between nations, facilitating the rapid exchange of actionable information on new and emerging threats, operational tactics and financial flows that sustain terrorist activities. By breaking down silos between domestic agencies and international partners, such initiatives would greatly enable the identification of patterns and linkages that might otherwise remain obscured. Even so, joint intelligence efforts empower nations to dismantle transnational networks through coordinated interventions, such as disrupting supply chains, targeting safe haven states, and apprehending key operatives - efforts that would have been obscured if a single intelligence entity were to take up the task of a counter-terrorism operation.

CASE STUDY #1

The 2008 Mumbai Attacks, 26/11[1]

26/11 marked a watershed moment in the history of global terrorism and underscored critical gaps in intelligence-sharing networks between India and Pakistan. A relationship that can be explored and critiqued in detail within the committee. These attacks, executed by ten operatives of the Pakistan-based terrorist group Lashkar-e-Taiba (LeT), paralyzed India's financial hub for nearly four days, claiming the lives of 166 people and injuring hundreds more. Beyond the human and material toll, the tragedy exposed significant deficiencies not only in regional state-level intelligence coordination but also in international intelligence coordination between the agencies in Pakistan and India. Not only was this further obscured by the geopolitical tensions between the nations, but the dynamic of Lashkar-e-Taiba being a state-sponsored group also caused India to be hesitant to coordinate with the Pakistani intelligentsia to officiate an adequate investigation into the attacks.

These attacks were meticulously planned over several months and involved rigorous training, reconnaissance, and the utilization of modern communication technologies. Pakistani intelligence agencies, primarily the Inter-Services Intelligence (ISI), have long been accused of harbouring and supporting the LeT - even to the point of the 26/11 operatives admitting to meeting with high-ranking ISI officials and using ISI resources to gather crucial reconnaissance information. Subsequent investigations revealed that the attackers were in direct contact with handlers in Pakistan, throughout the operation - who provided real-time instructions via satellite phones and

[1] https://www.britannica.com/event/Mumbai-terrorist-attacks-of-2008

other voice-over-internet protocol (VoIP) systems. This sophisticated command-and-control system highlighted the role of a well-established terror infrastructure, which eventually raised serious questions about the extent of Pakistani state complicity, or at the very least, negligence within Pakistan's intelligence apparatus.

In the leadup to the attacks, numerous intelligence warnings could have potentially averted the disaster, but systemic failures and a lack of actionable intelligence sharing between India and Pakistan rendered these ineffective. India's main intelligence agency, the Research and Analysis Wing (RAW), and the Intelligence Bureau had received scattered inputs from both domestic sources and international partners, including counterparts within the US, about a potential maritime threat, and the possibility of a LeT operation targeting Mumbai. It is crucial to understand that the coordinated planning of terror attacks across borders cannot happen so covertly, to the point where intelligence agencies are completely unable to pick up on hints and clues. However, the warnings that were intercepted were either too vague or inadequately acted upon. For instance, in September of 2008, the US reportedly informed Indian authorities about a possible LeT plot involving sea routes in and out of Mumbai, but the absence of an integrated response mechanism allowed the terrorist to exploit intelligence vulnerabilities and pounce on the opportunity to launch their attack in November of the same year.

On the Pakistani side, the ISI's alleged dual role as both an intelligence-sharing agency and a supporter of proxy warfare against India further undermined any possibility of regional intelligence cooperation. Now whilst Pakistan has officially denied involvement in the attacks, subsequent evidence including the interrogation of captured attacker Ajmal Kasab, revealed direct links to Pakistani handlers. The reluctance of the ISI to crack down on groups like LeT within their domestic jurisdiction, despite international pressure, reflects a broader strategy of using such groups as strategic assets, thereby eroding any semblance of trust between the two nations and complicating any meaningful intelligence exchange. While we can debate the extent of Pakistani state influence on LeT's operation, it is possible to make an objective judgement about whether the ISI supports LeT at all - and the resounding yes makes it ever more difficult for the nation to reconcile with India, and partake in constructive intelligence sharing operations to enhance the nation's capabilities specifically in counter-terrorism efforts.

Back over in India, in the aftermath of 26/11, many of the domestic intelligence mechanisms underwent significant change and alternation - promising reform which seemed to have enhanced the nation's capabilities to intercept terrorist cells and prevent attacks in future. Such reforms were as follows;

1. The passing of the **National Investigation Agency Act of 2008[2],** which officially established the NIA, a specialized federal agency with the mandate to investigate and prosecute offences specifically related to terrorism and national security. This significantly streamlined the judicial process of accountability and investigation once the intelligence agencies gather information and data regarding a specific operative or group, The NIA operates with jurisdiction across states, ensuring swift investigation without procedural delays caused by inter-state jurisdictional issues,

[2] https://www.mha.gov.in/sites/default/files/2022-08/The%2520National%2520Investigation%2520Agency%2520Act%2C%25202008_1%5B1%5D.pdf

2. The **RAW and IB were restructured,** with greater operating emphasis on new advancing protocols, technological surveillance, and human intelligence - largely through the form of HUMINT. Moreover, coordination between RAW and IB was improved to address intelligence gaps, especially considering that RAW collected external intelligence - whilst IB collected domestic intelligence. The increased coordination between the two agencies meant that it was easier to parse foreign and domestic intelligence with one another, leading to more swift interceptions of potential attacks and threats,
3. The **Multi-Agency Centre** within the Intelligence Bureau was revamped to enhance information sharing amongst different agencies, including state-level and federal bodies. Subsidiary MACs were set up in states to facilitate better coordination between central and state intelligence units. As opposed to a fixed network sharing method, these MACs adopted network fusion systems where a combination of various networks was used, which best-facilitated intelligence sharing on a multi-level basis.

Further Reading

In contrast to the PD2 topic, PD1 offers a more technical and practical aspect to the debate regarding the core operating principles and structures of intelligence agencies. Exploring the various organizational reforms around intelligence agencies will definitely help understand the operating models of your own intelligence agency - going all the way from the types of intelligence-sharing networks to the fields of shared intelligence across a country's government and bureaus.

In general, there are four main types of intelligence-sharing networks according to the *Homeland Security Affairs,* a journal for the Department of Homeland Defense and Security[3]. These are as follows;

1. **Hub-and-spoke** networks where intelligence sharing involves a common connection to intelligence and information usually through a common hub from which all relevant authorized members can access them. These types of models are especially common in US federal intelligence services, and is evident in the deployment of *Intellipedia*[4] used by the US Intelligence Community,
2. **Co-located liaison** networks involve the creation of cooperative, multi-agency or multi-governmental locations which house representatives and analysts from a diverse set of agencies. These operate as dedicated organizations/buildings in larger governmental structures to facilitate intelligence sharing. An example of this is located in the US through the form of *fusion centres*[5]*,* which forms a decentralized self-organizing network of intelligence offices that coordinate with one another to share information from both non-law enforcement bodies and law-enforcing bodies,
3. **Hierarchical linear** networks involve singular, point-to-point connections between agencies such as between a federal or state-level organization, or from a state organization to a local entity. These mechanisms tend to be extremely slow, but come with the added benefit of tightened security as this form of exchange is highly controlled and coordinated,

[3] https://www.hsaj.org/articles/232
[4] https://youexec.com/questions/what-is-intellipedia-and-how-has-it-become-a-key-resour
[5] https://www.wikiwand.com/en/articles/Fusion_center

4. **Fused** networks are essentially a dynamic combination of the three options above, where different systems are deployed in certain circumstances to best adapt to the ongoing scenario or use case.

Intelligence collection in counter-terrorism encompasses a variety of methods, each uniquely suited to address different facets of the threat itself. **HUMINT**, derived from human sources, plays a vital role in penetrating terrorist networks, particularly those that operate in decentralized or clandestine cells - such as those prominent amongst ISIS and Al-Qaeda. Conversely, **SIGINT**, which involves the interception of electronic communications, has been increasingly pivotal in identifying operational patterns, logistical arrangements - and most importantly, the recruitment strategies of modern terrorist organizations that rely heavily on digital platforms. The current state of intelligence-sharing agreements between nations often ignores the benefits provided by **OSINT**[6], whose open-source nature allows for far more flexible and thorough dissemination of online activity. Not only is such a method significantly more cost-effective for agencies, but it also allows for agencies to engage in more transparent and dynamic information sharing with other agencies, either internationally or between domestic offices.

Over the years, various international agreements and alliances have been specifically established to facilitate intelligence sharing in counter-terrorism - each reflecting the evolving threat landscape and geopolitical dynamic. One of the most well-known of such alliances is the **Five Eyes**[7], which exemplifies high-trust intelligence sharing between its member states. Not only does it act as a model for other future potential intelligence-sharing communities, but the specific protocols and networks established between the member states can be scrutinized and tweaked to fit other scenarios elsewhere. This agreement, born out of necessity following the Cold War, has expanded significantly to address modern security challenges - including terrorism, by pooling SIGINT and coordinating counter-terrorism operations, such as coordinated busts and raids of active sleeper cells in foreign states.

[6] https://www.wikiwand.com/en/articles/List_of_intelligence_gathering_disciplines

[7] https://www.wikiwand.com/en/articles/Five_Eyes

PRACTICE DEBATE 2: Reforming Intelligence Agencies to Maintain Ethical Practices with Emphasis on Politicization

Background and Context

The question of “ethics” within intelligence activities is often muddled in historical examples of the gross misinterpretation of intelligence reports, and the overt neglectfulness towards ensuring respect for civilian freedoms and rights. In light of recent geopolitical developments, and the subsequent rise of extremism post-9/11 era - the intersection between intelligence gathering and the pursuit of political and geopolitical agendas has only grown larger. Its roots set in the Cold War - most notably the successful (yet drastically detrimental) efforts by the CIA in toppling both the democratically elected governments in Iran (in 1953) and in Chile, where the CIA propped up notorious dictator General Pinochet in 1973. The rate of such occurrences has only grown tremendously in recent years and has thus allowed various intelligence agencies to uncompromisingly violate the sovereign integrity of many third-party nations.

It is in this intersection, that the dilemma arises regarding the safeguarding of civilian freedoms and rights - in line with supposed “ethical practices”. To what extent are personal freedoms allowed to be violated, in the pursuit of intelligence gathering and other relevant intelligence operations? This very question has caused tremendous controversy, especially concerning the American response post-9/11 and the domestic mass surveillance programs initiated by the NSA under the Presidency of George Bush. Whilst the CIA can have an extensive “Code of Ethics”, it does not completely rule out the possibility of abuse and due negligence when it comes to occurrences of civilian violations.

Within this specific section of the study guide, the case study will specifically explore the intelligence apparatus of the US and its strategic missteps in relevance to the topic. However, this is not to say that debate or discussion in committee should be confined to the context of the US alone. Other specific instances of overt politicization include, but are not limited to;

a. The **UK’s** *Dodgy Dossier* of 2002 which asserted the existence of WMDs in Iraq,
b. The use of *Pegasus spyware* by the **Saudi Arabian** government to monitor political opponents and activists (most prominently Jamal Khashoggi),
c. The misuse of *Pegasus spyware* by the **Israeli** government and its intersection with targeting dissenters amidst political turmoil over judicial reforms in 2023,

Further points of reading as a preemptive to understanding the context of the case study and the discussion points later on;

1. https://www.jstor.org/stable/20031908
2. https://politicalviolenceataglance.org/2017/12/19/how-does-intelligence-become-politicized/
3. https://warontherocks.com/2015/09/on-the-politicization-of-intelligence/
4. https://classic.austlii.edu.au/au/journals/MonashULawRw/1988/4.pdf

CASE STUDY #1

The aftermath of 9/11 marked a transformative era for the US intelligence apparatus, by reshaping their mandates, expanding their operational scope, and increasing the political scrutiny of their activities. Whilst these shifts were intended to bolster state security, they also exposed blaring vulnerabilities to politicization, particularly in two instances; the justification for the 2003 Iraq Invasion and the NSA's mass surveillance programs emanating from the Bush era. Both these cases illustrate how political agendas can often distort intelligence, undermine public trust, and compromise the ethical principles that should otherwise guide the operational activities of such agencies.

The US intelligence apparatus in the 2003 Iraq Invasion

In the leadup to the 2003 Iraq Invasion, the administration under George W. Bush relied heavily on intelligence reports to justify any such use of military intervention. The central claim was that Saddam Hussein's Iraq possessed weapons of mass destruction and had maintained links to terrorist organizations, including the likes of Al-Qaeda. Whilst these assertions were later discredited and heavily scrutinized by the international community, they nonetheless revealed a glaring issue of excess political influence on intelligence matters - which inevitably compromised the very objective nature of said intelligence reports and activities.

The CIA's "White Paper[8]" (on Iraq's WMD programs), released in 2002, became the Bush administration's cornerstone in the case for war. This report asserted that Iraq had an active WMD program, and was attempting to acquire materials for nuclear weapons. However, subsequent investigations, particularly the Iraq Survey Group's report[9] in 2004, adequately concluded that Iraq had dismantled its WMD program as of the early 1990s. The evidence used by the CIA to support the claims of "aluminum tubes" allegedly being used to make centrifuges was therefore concluded to be purposefully misinterpreted, to satisfy a certain narrative or bias. The process of producing this intelligence was deeply politicized - and analysts within the CIA and the DIA (Defense Intelligence Agency) have repeatedly reported that they had faced pressure to conform their findings to the administration's narrative. The Office of Special Plans[10], a unit established within the US's Department of Defense, was accused of bypassing traditional intelligence review processes to provide Congressional policymakers with selectively chosen or exaggerated intelligence This thereby created an echo chamber that reinforced pre-existing biases within policymakers, rather than presenting objective reports which could have otherwise painted a different picture about the security situation within Iraq.

The NSA's surveillance program

The NSA became a central player in the US government's response to the 9/11 Attacks, with its surveillance program being significantly expanded in terms of scope and mandate as a result of the PATRIOT Act of 2001. These programs, aimed at identifying and preventing terrorist activities, involved the mass collection of communications data from domestic US citizens primarily, as well as foreign nationals (although secondary nature). Whilst the initiatives were framed as "essential" for national security, they sparked controversy over the ethical and legal implications of mass surveillance - especially when details surrounding the program leaked to the general public in light of the 2013 Edward Snowden leaks[11] of the NSA.

[8] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB129/part10-whitepaper.pdf
[9] https://www.govinfo.gov/app/details/GPO-DUELFERREPORT
[10] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB456/
[11] https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

The politicization of intelligence within the NSA is evident in the way surveillance programs were both justified and implemented. The agency's flagship program; "PRISM", authorized under the Foreign Intelligence Surveillance Act of 1978 (and subsequent amendments), allowed the NSA to collect data directly from major tech companies like Google, Apple, and Facebook. Whilst initially a covert program, it came to public attention in the 2013 leaks - where internal documents revealed that the NSA had collected vast amounts of metadata, including phone records, emails, and online activity. It is most important to note, that such information was collected and stored without any warrants, or direct links to a possible terrorist "threat".

Politically, these programs were bolstered by a narrative of fear propagated by Congressional policymakers in the US. Intelligence findings were selectively used to highlight imminent threats, justifying expanded surveillance powers whilst they downplayed the risks to civil liberties. For example, senior officials frequently cited "disrupted plots", such as the 2006 transatlantic aircraft plot[12], to validate the effectiveness of the NSA's operational capabilities. However, subsequent reviews, including a 2014 report[13] by the Privacy and Civil Liberties Oversight Board (an independent executive agency established by Congress in 2004), found little evidence that mass surveillance played a decisive role in preventing such attacks. Whilst the "theoretical" threat of an attack could be subsided by more aggressive intelligence operations - it is very often that intelligence agencies often overestimate the level of aggressiveness necessary to tackle such a threat, which often leads to compromises on civilian liberties and freedoms.

Whilst the US Congress passed the USA FREEDOM Act in 2015 to curtail the NSA's surveillance powers by ending the bulk collection of phone records, and by increasing oversight - critics argued that these measures did not fully address the deeper issues of transparency and accountability, and the very mechanisms in the US that allows for Congressional policymakers to influence intelligence decisions - to the extent that it satisfies the political rhetoric of their own.

FURTHER READING

Within the context of PD2's debate, delegates must also be prepared to engage in constructive debate specifically regarding various reforms that can be implemented to ensure ethical practices and prevent overt politicization. The following points help find more nuanced points of discussion that are not mentioned in the case study above;

1. Transparent oversight mechanisms, with no compromise to operational secrecy
    a. Security sector reform (SSR) and good security sector governance (SSG) as foundational principles for intelligence operations[14],
    b. Importance of intelligence oversight and consequent administrational integrity
2. Whistleblower protections for political interference claims
3. Distinguishers and differentiators between national security threats, and domestic political dissent
4. Declassification protocols to prevent retrospective politicization
5. Ethical frameworks to prevent intelligence bias under political pressure

[12] https://www.wikiwand.com/en/articles/2006_transatlantic_aircraft_plot
[13] https://www.aclu.org/sites/default/files/assets/aclu_pclob2014-04.pdf
[14] https://thesecuritydistillery.org/all-articles/what-is-intelligence-oversight-and-why-does-it-matter

Considering that various intelligence agencies operate on varied principles and operating guidelines, **it is best to first understand how exactly your representative agency operates - in all aspects, especially regarding the position of said agency in the political structure of your country.** For example, Russia's FSB[15] primarily answers to the President and operates within the executive branch of the government. Only some administrative matters such as the budget or oversight are overseen by the Federal Assembly (the Russian equivalent of the parliament). **Understanding the operation of your agency will better help you identify the more nuanced operational differences between other agencies, and this will prompt further research and discussion into why or how certain operating principles are better, or why certain reforms are more effective etcetera.**

[15] http://government.ru/en/department/113/

MAIN CONFERENCE: The Consequential Influence of Intelligence Agencies on Modern Conflicts

Background and Context

As mentioned throughout the study guide, the influence of intelligence agencies in the sphere of global conflicts has only grown steadfast in recent times. They have become critical players in almost all modern-day conflicts, exerting significant influence via both overt and covert means. Originating as tools of statecraft, their roles evolved significantly during the Cold War, where the ideological context between superpowers drove the need for clandestine operations, espionage, and counterintelligence. However, their influence now far extends beyond that era, with their activities often functioning as instruments at the centre of shaping conflict dynamics - whether by disrupting adversarial networks, engaging in regime destabilization or facilitating proxy wars. Such instances are not without controversy, as they often straddle the fine line between ensuring national security and violating the sovereignty of other states - raising obvious questions of ethics and legality.

In the context of contemporary conflicts, the evolving nature of warfare has further enhanced the role of intelligence agencies to a great degree. Hybrid warfare - which integrates conventional military operations with cyber-tactics, propaganda and economic coercion to state a few, places intelligence at the forefront of conflict management. The growing use of artificial intelligence and greater cyber capabilities have also allowed intelligence agencies to broaden their scope of activities, in relevance to conflicts and disputes - allowing them to preempt and counter new and old threats. However, this expanded purview raises tremendous challenges, including misinformation campaigns, the weaponization of information against foreign states, and other instances of infringements on civil liberties. With modern-day conflicts becoming increasingly multidimensional, it is only apparent that intelligence agencies adapt and reform to become more indispensable in safeguarding state interests - with this apparent influence becoming more and more contentious in the global circuit as their methodologies and instances become public and known.

The main conference topic serves as the buildup in discussion based on the prerequisite debate following the two practice debates. The current global network that facilitates information sharing in combating terrorism, and the concerns regarding ethics all feed into the overarching influence and presence that these agencies have in the political and geopolitical spheres across the globe. As delegates, you must be able to derive the same research from previous topics and apply them readily to the main conference topic. Questions of whether it is important to regulate the influence of intelligence agencies, or debate on the issue of how conflict accountability affects intelligence agencies of third parties in proxy conflicts for example - are all well within discussion, and are immensely encouraged to be brought up during debate.

SPECIFIC ISSUES / PROBLEMS (Explored in detail)

As opposed to the earlier structure of the study guide, where specific case studies were given - the following content will include a more comprehensive overview of the existing problems, within the context of several examples and mini-case studies. It is important to understand that the conference topic covers a wide variety of different nations, and it is encouraged to pull examples from a multitude of various intelligence communities across the globe. That being said, it is also important to recognize that these examples have far-reaching consequences - all the way from the private sector of many nations, to the day-to-day activities of individual citizens. Keeping an open mind about the impacts of the operations of these intelligence agencies will allow you, as a delegate, to understand more nuanced levels of research and content.

Perhaps the most contentious issue at hand is the *question of responsibility and accountability by state actors* (in this case, intelligence agencies as the medium) in dispute and conflict scenarios. To provide a crude example; the sponsoring of separatist movements in the Donbas region of Ukraine, following the 2014 Euromaidan[16] protests, by the Russian state GRU[17] (Main Intelligence Directorate) and the FSB falls in line with the gross lack of accountability as mentioned earlier. The Russian intelligence apparatus repeatedly funded and allowed rebel groups[18] to operate within Russian borders, as the base to launch more coordinated attacks against Ukrainian garrisons along the border - providing tactical and logistical support to these groups as well. Furthermore, even with surmounting evidence to prove that the FSB and the GRU were complicit in the funding of separatist groups in Ukraine - no clear action was ever taken against the state. This specific instance highlights three things;

1. The **ease at which nations can now easily disguise geopolitical exertions of power, through covert means and the veil of ambiguity that intelligence agencies provide** (plausible deniability),
2. The **lack of adequate concerted information** to prove a **direct line of intent between the state and the actions conducted by these agencies,**
3. The concerning use of intelligence agencies as **proxies in asymmetric warfare against other nation-states,**

Furthermore, another contentious issue within the debate is the fact that *intelligence agencies are becoming increasingly embedded within the military-industrial complex of its host nation-state*. This inadvertently causes two things to shift within the strategies of these intelligence agencies in the modern era;

1. Their role is becoming **increasingly more present in the long-term**, with a focus on **strategic geopolitical objectives**, as opposed to **short-term intelligence collection objectives -** surrounding specific threats to foreign security,
2. The **assets and expertise of intelligence agencies** are being used **more frequently by the military command** of many nations, to further aggressive and soft militarization of new territories; either through forced coercion, or soft exertions of power (ie, China and Taiwan) To analyze the case of China v Taiwan, the South China Sea is the best example in which the Chinese state intelligence agency (the Ministry of State Security) has had external influence in coordinating with the People's Liberation Army - to preemptively position China in greater control over the disputed sea[19]. The MSS often collaborates with the PLA to gather and disseminate real-time intelligence on the movements of US and allied naval forces - and this alignment exemplifies how intelligence agencies now **actively shape military strategies, rather than merely supporting them**. A significant dimension of the MSS's activities with the

[16] https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests
[17] https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2322807#abstract
[18] https://pism.pl/publications/the-involvement-of-irregular-armed-groups-in-the-russian-invasion-of-ukraine
[19] https://www.rand.org/content/dam/rand/pubs/external_publications/EP60000/EP68058/RAND_EP68058.pdf?utm

> PLA lies in its role in economic and cyber espionage - which directly feeds into China's military-industrial complex. By specifically targeting Western defence contractors, the MSS has facilitated the theft of critical technologies, such as stealth fighter designs, missile systems and complex drone capabilities. For example, in 2018, Chinese hackers, "allegedly linked to the MSS" stole sensitive data from a US Navy contractor[20], including plans for a supersonic anti-ship missile. This systematic acquisition of advanced technologies (which had traits of being orchestrated by a nation-state), bolstered China's military capabilities to an extent, enabling it to field cutting-edge platforms such as the J-20 stealth fighter and several designs for hypersonic missiles.

It is quite intuitive to also point out that the US similarly engages in such activities, most especially in the realm of cyberespionage against private entities in nations like Russia and China. The aforementioned PRISM program deployed by the NSA also included an extensive espionage operation targeting Huawei Technologies (a telecommunications firm based in China that is closely associated with China's defence and intelligence apparatus) allegedly based on the "malicious use of 5G networks" by the Chinese government against Western targets[21]. What this highlights is a **gross lack of international accountability** for when intelligence agencies can launch wide-ranging espionage missions, that in some instances, can cause civilian harm and irreparable economic damage and consequences. One may argue that such concerns falter in the grand scheme of achieving political goals, with the consequences merely being inconsequential collateral. Others may argue that the advancement of covert espionage operations (within the broader context of military conflicts or disputes) is a highly ineffective instrument to advance foreign policy, and is highly inadequate in fulfilling the goals and obligations of intelligence agencies. Once again, the question of whether **support** or **coordination** between intelligence and military commands comes into play - this is especially evident in the US, where policymakers and intelligence officials have repeatedly made calls for greater degrees of separation, and more support-based intelligence strategies that avoid direct intervention into foreign disputes[22].

While it is obvious to assume that intelligence agencies play crucial roles within the umbrella of the military-industrial complex[23] - this role has become more apparent in recent years. Many nations have a strict separation of influence and power between the intelligence command and the military command, with both wings acting independently of each other, only answerable to the most senior position above (which in most instances, is the executive). This is evident in the UK, where both the MI6 and MI5 are "civilian-led organizations" which operate independently from the Ministry of Defense - drawing a clear line of separation, which on occasions, merge during specific military operations (with clear delineations of responsibility to ensure impartiality). On the opposite side of the spectrum, in countries like Russia - entities like the GRU operate entirely within the direct command of the Russian Armed Forces. Placing intelligence expertise and assets, within direct control of military officials in the country. Even though it is up for debate as to which method of operation is more beneficial, it is quite apparent that the latter often leads to greater instances of negative harm.

[20] https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html
[21] https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000
[22] https://www.everycrsreport.com/reports/96-844.html
[23] https://www.tandfonline.com/doi/full/10.1080/08850607.2023.2209493#d1e145

To contextualize the debate in more current affairs, the projection and decades-long planning of tampered explosive pagers by Mossad against Hezbollah officials and commanders in Lebanon[24] (and non-Hezbollah targets in Syria), is another example of how interconnected intelligence agencies are becoming in the field of military warfare and intervention against foreign forces. Within the broader dispute between Israel and Hezbollah in Lebanon, both sides have taken considerable action to leverage force against one another - with Israel's Mossad using covert strategies to wage an asymmetric war against Hezbollah. The coordinated explosion of pagers not only reflects a new era in the field of weaponization but also opens up questions of international legitimacy, as the detonation of these pagers breaches the laws of war and is indiscriminate - of which Amnesty International has reported several specific violations[25].

POINTS OF DISCUSSION

Building upon the content above, the following questions should give enough insight into the breadth of research that is necessary within the ISC. Keep note that

1. The integration of emerging technologies, and their use case in both decision-making processes, and the enactment of operations by intelligence agencies,
   a. Use of artificial intelligence to enhance data collection and analysis - and to identify patterns in collected data to provide more actionable insights, thereby greatly improving the decision-making processes that intelligence agencies often have to make during operations, https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection#:~:text=Emerging%20technologies%2C%20particularly%20AI%2C%20advanced,signals%20detection%2C%20and%20target%20identification.
2. The role of intelligence operations in shaping up narratives through propaganda strategies,
   a. Like the Russian government's use of disinformation in its strategy, within regions like Georgia[26] (largely in 2008) and Ukraine. These disinformation campaigns, launched by the FSB, aim to manipulate public perception and to shape political dynamics to satisfy the pro-Russia narrative within predominantly Ukrainian territories, https://publications.armywarcollege.edu/News/Display/Article/3789933/understanding-russian-disinformation-and-how-the-joint-force-can-address-it/
3. The influence of intelligence agencies in propelling the arms trade, and in several instances - enabling it to thrive under the military-industrial complexes of nation-states,
   a. Defence contractors and technology companies, such as Lockheed Martin and Northrop Grumman in the US, develop and supply advanced systems and software used in intelligence operations. This collaboration between agencies and private industry contributes to the growth of the military-industrial complex, which many see as detrimental to the state itself,

[24] https://edition.cnn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intl/index.html

[25] https://www.amnesty.org/en/latest/news/2024/09/lebanon-establish-international-investigation-into-deadly-attacks-using-exploding-portable-devices/

[26] https://www.chathamhouse.org/2022/03/georgia-must-bolster-resilience-information-warfare

    https://www.maris-tech.com/blog/technology-and-intelligence-gathering-innovations-maris-tech/?utm

4. The role of intelligence agencies in orchestrating political dynamics in foreign countries, especially during times of conflict,
    a. The CIA has historically engaged in covert operations to influence political outcomes in foreign nations - obvious examples include Iran, Chile and Libya
5. The efficacy, or even the existence of mechanisms to ensure oversight of intelligence agencies that leads to external collateral damage of third parties,
6. The rise of non-state actors - such as private intelligence firms and cyber-mercenaries, in intelligence activities within conflict situations,