G20

TOPIC A: Development of the India – Middle East– Europe, Economic Corridor (IMEC)

TOPIC B: Digital Economy and Cybersecurity

Language: English

G20

Authors:Tejas Raman Wattamwar

Time For Opening Speech: (90 seconds)

One opening speech regarding both topics

DESCRIPTION OF THE COMMITTEE:

The Group of Twenty or "G20" is a premier and main informal forum, with its main alignment and main objectives being international economic cooperation and strengthening global economic ties and cooperation. It plays an important role, defining and establishing and worldwide architecture and management to all major international economic issues. Each year the G20 rotates through the presidency the G20 presidency is occupied by one state actor each year from December 1, 2023, until November 30, 2024. The presidency is occupied by the federative Republic of Brazil. The Previous president of the G20 summit for the majority of 2023 was held by the Republic of India. The G20 was established in 1999 after an Asian financial crisis, where the United finance, ministers, and central bankers from the 20 largest and emerging economies in this global crisis. did G20 was not as active after his financial crisis, but it reinstated its objectives, and the organization became active again after the 2008 housing crisis. The members of the G20 include Argentine Republic, Australia, federative, Brazil, Canada, Republic of China, French, Republic, federal, Republic of Germany, Republic of India, Indonesia, Italy, state of Japan, Korea, United, Mexican states, the kingdom of Saudi Arabia, South Africa, Russian Federation, Turkey, United Kingdom of Great Britain, and Northern Ireland, United States of America, and two regional bodies being the African Union, the European Union.

TOPIC A: Development of the India – Middle East– Europe, Economic Corridor (IMEC)

HISTORICAL CONTEXT

Historical context for the economic order between India, Middle East, and Europe is replicating a historical trading link between the Indians of continent middle east, and Eurasia. This was usually done through the Silk Road, as well as other Nevo corridors. Historically these historical quarters were essential for spice, trade, gold, trade, and many others between these different continents, this is what brought many of the languages economies and others towards the Middle East as was the influence it had on Europe. All of these quarters were broken when the British Raj, colonized India, and many parts of Middle East later on the British, Raj was named British India, and after 200 years of colonizing in 1947 one India got independent. These corridors were never again established because of political and economical problems in the region.Later on in the 1990s Delhi had been experimenting with socialist strategies of import substitution and self-sufficiency, but because of the social reform and economic reform, came to force this caused Delhi to explore new connect activities with the west, especially with markets in Europe, sparking interest in easier connectivity links to the west, especially bypassing its neighbors, such as Pakistan for years this was not possible as Pakistan blocked all proposals and access towards the Arabian gulf not making this possible. so why this problem India decided to reach out to Iran Dhaiya was that India could use the Jabbar port by reaching into Afghanistan, and then from the international north south transport corridor reach central Asia, Russia, and Europe. The plan was perfect on paper, but because of the different problems and conflicts between Iran and United States in their frosty relation was not possible as United States is most important trade partner, and this removed India's desire, and possibility to create a corridor between India and Eurasia, as well as Europe.

CAUSES

The creation of the Indian Middle East Europe Carder is to improve cohesion and reshape the global trader routes in this the eighth Saenz account alone for 40% of the world population and almost 50% of the world economy by changing the trade routes making the more efficient key commercial hubs and development of clean energy energy telecommunication network and enhancing Internet access would increase as well as transportation around Asia Europe and Mali will increase although these can also cause a dual political stability for neighboring countries of the member states such as Pakistan, Iran, China, Yemen, Syria, Iraq, and many others, which depend on these trade outs from many parts of the economy this is a political advantage for many countries, and is also the reason why many countries do not want the economic trade out to happen objectives of the economic to reduce cost promote economic equation, free jobs, cut greenhouse, gas emissions, and improve the global infrastructure for investment.

REPERCUSSIONS

ECONOMIC IMPACT (Trade Dynamics):

The formalization of the India-Middle East Economic Corridor in theory has many economic benefits nevertheless, the implementation of such a corridor may also yield unintended consequences, particularly for nations heavily reliant on revenue generated from the taxation of maritime traffic through the Gulf of Aden. These countries, often situated along the strategic waterway, have historically leveraged their geographical position to levy tariffs and fees on ships passing through their territorial waters. This revenue stream plays a crucial role in sustaining their economies, funding public services, and supporting essential infrastructure projects.

With the establishment of a more direct and efficient maritime route via the India-Middle East Economic Corridor, the demand for maritime transportation through the Gulf of Aden could diminish. As a result, the income derived from ship passage taxation may decline, posing significant challenges for the affected countries' fiscal stability and economic sustainability. This reduction in revenue could potentially impede their ability to invest in crucial sectors, address socioeconomic disparities, and maintain geopolitical influence in the region.

Furthermore, the reconfiguration of trade routes and economic dynamics brought about by the corridor may redistribute power and influence among participating nations. Countries traditionally dominant in maritime trade and transportation may witness a shift in their economic centrality, while emerging players along the corridor could rise in prominence. This reshaping of geopolitical dynamics could have far-reaching implications for regional alliances, security arrangements, and diplomatic relations. The following nations will face the most consequences include nations such as Yemen, Djibouti, Somalia, Pakistan and Iran.

IDEOLOGICAL IMPACT:

Following the establishment of the India-Middle East-Europe corridor, a seismic shift in geopolitical dynamics is anticipated, heralding both opportunities and challenges for nations across the region. This transformative initiative is poised to streamline trade, bolster economic cooperation, and foster connectivity between India, the Middle East, and Europe, ushering in a new era of commercial integration and regional collaboration.

However, alongside the promising prospects lies the looming specter of diminished influence for certain countries that have historically wielded ideological or strategic significance in the region. Traditional powerhouses may find their once-unassailable positions challenged as the corridor reshapes trade routes, economic alliances, and diplomatic alignments. With the focus shifting towards the efficiency and convenience offered by overland transportation, maritime chokepoints and traditional sea routes may witness a decline in strategic importance, thereby altering the geopolitical calculus of nations reliant on their control or proximity to these maritime arteries.

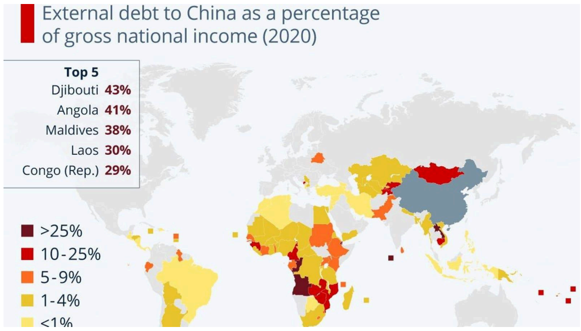
CURRENT SITUATION

The Belt and Road Initiative:

The Belt and Road Initiative (BRI), unveiled by the People's Republic of China in 2013, represents one of the most ambitious and expansive economic development projects of the 21st century. Encompassing a vast network of infrastructure, trade, and investment projects, the BRI aims to foster greater connectivity and cooperation among participating nations across Asia, Africa, Europe, and beyond.

At its core, the BRI seeks to revive and modernize the ancient Silk Road trading routes, which historically facilitated the exchange of goods, ideas, and cultures between East and West. Through a combination of infrastructure development, trade agreements, and financial investments, China aims to create a seamless network of transportation, energy, and telecommunications links, spanning land and sea.

The BRI's scope is truly staggering, with approximately 154 countries and international organizations either directly involved or expressing interest in participating. This expansive membership underscores the global significance and appeal of the initiative, which promises to stimulate economic growth, alleviate poverty, and promote regional stability through enhanced connectivity and cooperation. One of the primary motivations behind the establishment of the India-Middle East Economic Corridor (IMEC) was to provide a strategic counterbalance to the growing influence exerted by nations like the People's Republic of China through their ambitious Belt and Road Initiative (BRI). Recognizing the transformative potential of the BRI in reshaping global trade networks and geopolitical alignments, stakeholders within the India-Middle East region sought to assert their own economic interests and enhance their collective bargaining power on the world stage. Even though the BRI has 154 member states many of the projects have not been completed and are under construction as well many countries are 100 year debts to Chinese companies and the government for many of the infrastructure project for example the



Countries external debt to China (Retrieved from Forbes.com)

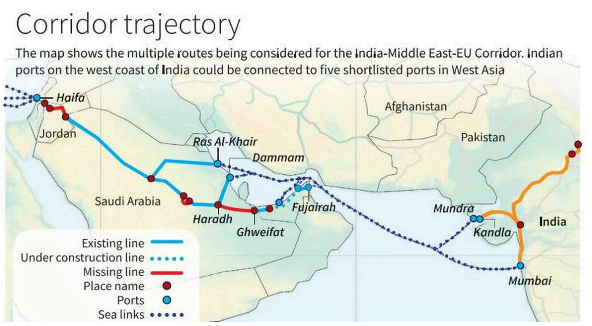
Infrastructure Creation:

One of the main obstacles to the development of the India-Middle East Economic Corridor (IMEC) is the lack of infrastructure required to carry out the project's intended goals. This ambitious project is naturally split into two main parts, each of which has its own set of challenges and complexities: the creation of new ports and maritime routes to guarantee the best possible supply chain logistics efficiency, as well as the new railway connections that will link the United Arab Emirates, Saudi Arabia, Jordan, and Israel.

First and foremost, significant funding for port infrastructure, navigational systems, and maritime security measures is required to address the marine portion of the corridor. The construction of new ports strategically situated along the corridor and the improvement of existing ones are necessary for the effective transit of products via sea routes.

Modern infrastructure and technology are required at these ports in order to handle growing cargo volumes, expedite customs processes, and guarantee seamless transit for ships sailing the area's seas.

Concurrently, constructing strong rail networks to link important economic centres in the United Arab Emirates, Saudi Arabia, Jordan, and Israel poses a significant logistical and engineering challenge. To enable seamless cross-border transit, this massive project calls for the building of new train lines, the renovation of current infrastructure, and the installation of interoperable technology. Governments, private investors, and international players must work closely together to overcome geographical obstacles, navigate regulatory frameworks, and get money for such large-scale railway projects.



Corridor trajectory

The map shows the multiple routes being considered for the India-Middle East-EU Corridor. Indian ports on the west coast of India could be connected to five shortlisted ports in West Asia

India-Middle East-Europe Economic Corridor Proposed Route
(Retrieved from thehindu.com)

Conflict in the Middle East:

Another significant limitation facing the development of this corridor stems from the persistent military conflicts plaguing the region. Examples include the longstanding Israel-Gaza conflict, the ongoing conflict between Houthi Rebels and the United States and the United Kingdom, and the tensions between Iran and militants in the Middle East. These conflicts create an environment of instability and insecurity, posing considerable risks to the establishment of ports, railways, and other infrastructure necessary for the corridor's operation. The ongoing violence and military engagements not only disrupt construction efforts but also raise concerns about the safety and security of trade routes passing through these conflict zones.

Moreover, the volatile nature of these conflicts can deter governments and investors from committing resources to the corridor's development. The prospect of investing in infrastructure projects situated in or adjacent to conflict-prone areas may be perceived as too risky or politically sensitive, leading to delays or hesitations in funding and implementation. Additionally, the uncertainty surrounding the security situation in these regions may prompt stakeholders to reconsider their involvement in the project altogether, further undermining efforts to advance the corridor's construction and operation.

Furthermore, the instability and insecurity associated with these conflict zones can divert the attention of governments and investors to alternative routes or locations deemed more secure and conducive to trade and investment. Competing corridors may emerge as viable alternatives, offering safer and more stable environments for goods and trade to pass through. As a result, the geopolitical dynamics of the region, exacerbated by ongoing conflicts, may hinder the realization of the corridor's potential and necessitate careful consideration of security risks and strategic interests in its planning and implementation.

OBJECTIVES OF THE COMMITTEE

The committee's two main aims are to carefully weigh the possible advantages and disadvantages of pursuing this project, carefully determine whether it is feasible, and carefully map out future objectives. This thorough assessment seeks to not only ascertain the project's feasibility but also to pinpoint any obstacles and possibilities that might emerge during execution. The committee may make well-informed decisions about the proposed corridor's growth and guarantee that it is in line with national interests and overarching strategic objectives by carefully examining every part of it.

In addition to evaluating the project's feasibility, the committee is tasked with exploring alternative solutions or routes that may better serve the region's economic and geopolitical needs. This involves conducting thorough analyses of potential alternative corridors, considering factors such as geopolitical stability, security risks, infrastructure requirements, and economic viability. By examining a range of options and scenarios, the committee can identify potential fallback strategies or contingency plans to mitigate risks and optimize outcomes. This strategic approach enables the committee to adapt flexibly to changing circumstances and pursue the most advantageous path forward, whether it involves advancing the current project or pursuing alternative solutions that better align with regional priorities and objectives.

GUIDING QUESTIONS

1. How is your delegation related to the creation of this corridor?

2. Is your delegation part of the Belt and Road Inative or the India-Middle East-Europe Corridor?

3. What is your country's relation with the US or China?

4. What is the ideological stance of your delegation?

5. What is the economic situation of your country after WWII?

6. Who were the leaders of the United States and Soviet Union during the Cold War?

GLOSSARY:

- **Economic Corridor:** A geographical area or route designed to facilitate economic development and trade by connecting various regions through infrastructure, transportation, and trade facilitation measures.

- **Geopolitical Dynamics:** The interactions between political, economic, and strategic factors that shape the behavior of states and influence international relations within a specific geographic region.

- **Trade Facilitation:** Measures and initiatives aimed at streamlining and simplifying the process of importing and exporting goods, including customs procedures, border controls, and trade documentation requirements.

- **Stakeholders:** Individuals, organizations, or entities with a vested interest or involvement in a particular project, initiative, or issue, including government agencies, businesses, civil society groups, and local communities.

- **Supply Chain:** The network of organizations, resources, activities, and technologies involved in the production, distribution, and delivery of goods and services to end-users or consumers.

- **Investment:** The allocation of financial resources (capital) to acquire assets or undertake projects with the expectation of generating future income or returns.

- Multimodal Transportation: The transportation of goods or passengers using multiple modes of transport (e.g., road, rail, air, sea) within a single supply chain or logistics network to optimize efficiency and cost-effectiveness.
- Sustainable Development: Economic development that meets the needs of the present without compromising the ability of future generations to meet their own needs, balancing economic, social, and environmental considerations.
- Public-Private Partnership (PPP): A collaborative arrangement between government entities and private sector organizations to finance, develop, and operate infrastructure projects or provide public services, with shared risks and responsibilities.
- Global Value Chains: Networks of interconnected production and distribution activities spanning multiple countries and involving various firms, suppliers, and service providers in the production of goods and services for global markets.
- Risk Management: The process of identifying, assessing, and mitigating potential risks and uncertainties that may affect the successful implementation or operation of a project, initiative, or business venture.

- **Intermodal Transport:** The coordinated movement of goods using multiple modes of transportation within a single journey, often involving seamless transfer and integration between different modes (e.g., from ship to train to truck)

SUPPORTING LINKS

- Haidar, M. P. (2023, September 17). *India-Middle East-EU corridor to have multiple routes, but hurdles remain*. The Hindu. https://www.thehindu.com/news/national/india-middle-east-eu-to-have-multiple-routes-but-hurdles-remain/article67315835.ece
- Buchholz, K. (2022, August 19). The countries most in debt to China [Infographic]. *Forbes*. https://www.forbes.com/sites/katharinabuchholz/2022/08/19/the-countries-most-in-debt-to-china-infographic/?sh=9a23e5261d8c
- *History repeats: A new (old) economic corridor emerges*. (n.d.). Lowy Institute. https://www.lowyinstitute.org/the-interpreter/history-repeats-new-old-economic-corridor-emerges
- Gülten, Z. T. (2023, October 5). *The importance and goal of the India-Middle East-Europe Economic Corridor*. ANKASAM | Ankara Center for Crisis and Policy Studies. https://www.ankasam.org/the-importance-and-goal-of-the-india-middle-east-europe-economic-corridor/?lang=en#_ednref5
- ELDoh, M. (2023, September 26). *The India-Middle East-Europe Corridor: Challenges ahead | Geopolitical Monitor*. Geopolitical Monitor. https://www.geopoliticalmonitor.com/the-india-middle-east-europe-corridor-challenges-ahead/

- Nicolas Rapp Infographic Design Studio - Freelance Designer. (2023, March 8). *A map of sea shipping routes – Nicolas Rapp Design Studio*. https://nicolasrapp.com/studio/portfolio/the-shipping-news/

TOPIC B: Digital Economy and Cybersecurity

As time cases and technology advances there is a shift which many economies are facing and this is shift can be seen into the transfer into digital economies in which digital payments, data analytics and many more technological aspects towards commerce is shifting online, this fundamental shift and this b rings new threats towards payments and the digital industry in the form of cybersecurity. Cybersecurity and the digital economy have always been perceived by the governments in a one or two-dimensional view only looking at it from modification rather than a massive change bringing new threats to the sovereignty to nations and its people.

HISTORICAL CONTEXT

The introduction of early computing systems and the creation of mainframe computers in the 1950s and 1960s marked the beginning of the digital economy. But the digital economy didn't start to take shape until the 1980s, when personal computers became widely used, and the 1990s, when the internet started to become more commercially viable. The current digital economy was established by the widespread use of e-commerce, online banking, and digital communication platforms, which changed how consumers and businesses interacted

Strong cybersecurity measures were necessary to guard against new risks as the digital economy grew. The earliest examples of cyberattacks and the spread of computer viruses in the 1970s gave rise to the idea of cybersecurity. As phishing scams, malware, and data breaches became more complex over the next few decades, cybersecurity had to adapt as well.

The invention of antivirus software in the 1980s, the development of encryption technologies in the 1970s, and the emergence of specialised cybersecurity organisations and standards bodies in the 1990s and 2000s are significant turning points in the history of cybersecurity. Increased cybersecurity efforts were also spurred by the terrorist events of September 11, 2001, which resulted in the passage of laws like the USA PATRIOT Act and the establishment of agencies like the Department of Homeland Security.

The digital economy has grown in recent years due to the emergence of cloud computing, mobile technology, and the Internet of Things (IoT), which has also brought up new cybersecurity challenges. Cyberattacks are becoming more common and sophisticated, with disastrous results as they target people, companies, and vital infrastructure.

CAUSES

The main reasons for the existence of areas such as cybersecurity stem from several key factors, including global interconnectivity, the increased digitization of critical infrastructure, shortages in cybersecurity skills and expertise within the industry, regulatory compliance requirements, and various other factors such as rapid technological advancement.

Stuxnet:

When Stuxnet was identified in 2010, state-sponsored cyberwarfare entered a new phase. Stuxnet was a revolutionary cyberweapon. It was directed towards Iran's nuclear programme, specifically its facilities for enriching uranium. Stuxnet was painstakingly designed to get into and mess with centrifuge control systems, which are essential for enriching uranium to levels appropriate for producing nuclear power or possibly even for developing bombs. In order to impede Iran's progress towards obtaining nuclear capabilities, Stuxnet targeted these centrifuges with the intention of undermining its nuclear goals by resulting in bodily harm and operational setbacks. The intricacy and refinement of Stuxnet's architecture demonstrated a degree of technological know-how and resources more commonly linked to nation-state actors than to lone hackers or criminal groups.

Although the United States and Israel are credited with working together to create and implement Stuxnet, official statements about its origins remain silent. The goal of this clandestine effort was to thwart Iran's nuclear programme in order to avoid using overt military force, which might have sparked more regional unrest and instability. Due to Stuxnet's demonstration of the potency of cyberweapons as instruments of coercion and geopolitical influence, warfare underwent a strategic change. The fact that it was able to breach Iran's nuclear infrastructure and cause damage only served to highlight how important cybersecurity is becoming for both international and national security in the digital age.

The public revelation of Stuxnet and its subsequent discovery sparked intense debate over the morality, legitimacy, and ramifications of state-sponsored cyberattacks. Discussions over the proper conduct in cyberspace, who is responsible for cyberattacks, and if international conventions and accords are necessary to control cyberwarfare were spurred by it. Stuxnet also acted as a wake-up call for governments and organisations throughout the globe, emphasising how susceptible key infrastructure is to cyberattacks and how important it is to fortify cybersecurity measures in order to reduce the likelihood of such assaults in the future.

<u>Equifax Data Breach(2017):</u>

The 2017 Equifax data breach rocked the financial sector, affecting millions of customers and bringing attention to the serious dangers involved in handling sensitive personal data. The breach revealed the personal data of over 147 million customers, including Social Security numbers, birth dates, and addresses. It was caused by an Equifax system vulnerability that was not patched. Due to the widespread release of private information, people are now more susceptible to fraud, identity theft, and other nefarious actions. Following the incident, the public, legislators, and authorities put Equifax under intense scrutiny. One of the biggest data breach settlements in history, the incident resulted in multiple lawsuits, governmental investigations, and a $700 million settlement with the Federal Trade Commission. Companies all over the world were reminded by the Equifax hack to give cybersecurity and data protection procedures top priority in order to preserve customer information and uphold confidence.

Mt.Gox Bitcoin Exchange Hack(2014):

The 2014 Mt. Gox Bitcoin Exchange Hack stunned the cryptocurrency community and made clear the flaws of centralised exchanges. Following the theft of about 850,000 bitcoins, worth over $450 million at the time, Mt. Gox, previously the leading participant in the Bitcoin exchange market, filed for bankruptcy. The attack caused significant financial losses for consumers and permanently eroded trust in the security of bitcoin exchanges. It was linked to flaws in Mt. Gox's infrastructure and purportedly mishandled. The event brought to light the dangers of centralised exchanges, where users put their money to unaffiliated platforms, and emphasised how crucial it is to employ security precautions like multi-signature wallets and cold storage to safeguard digital assets. The cryptocurrency industry learned its lesson from the Mt. Gox hack, which led to a greater emphasis on security and regulatory compliance in order to stop such breaches and safeguard investors' interests.

REPERCUSSIONS

Economical Implications:

Digital economies have enormous economic ramifications that spur innovation, growth, and market expansion. Digital technologies have brought about a transformation in conventional businesses and facilitated the growth of novel sectors, including the sharing economy, digital banking, and e-commerce. Due to these changes, productivity has increased, efficiency has improved, and new business opportunities have arisen, driving economic activity to previously unheard-of heights. However, cybersecurity is becoming a bigger problem as digital economies grow quickly. Businesses and organisations are exposed to serious dangers from cyberattacks, data breaches, and other harmful acts, which can lead to monetary losses, harm to their reputation, and legal repercussions. Consequently, in order to defend against ever-evolving cyber threats and preserve the integrity of digital transactions, businesses all over the world are devoting resources to fortifying their cybersecurity defences and compliance protocols.’

Cybersecurity incidents can also have far-reaching effects on investor confidence, consumer trust, and market stability.

Cyberattacks and high-profile data breaches have the potential to undermine industry and business trust, which lowers customer confidence and brand loyalty. This erosion of trust has the potential to cause market disruptions, impact investor mood, and heighten volatility and unpredictability. Businesses need to prioritise cybersecurity and show that they are committed to safeguarding consumer information and privacy in order to reduce these risks. As governments put policies in place to handle cybersecurity risks and safeguard vital infrastructure and national security, regulatory compliance with cybersecurity laws and regulations is also crucial. In general, resolving cybersecurity issues is essential to preserving resilience, trust, and confidence in the digital economy, guaranteeing its continuous expansion and success in the years to come.

Political Implications:

Wide-ranging political ramifications of cybersecurity and the digital economy include a restructuring of international relations and governance frameworks. Governments from all around the world are debating whether or not to regulate the digital economy in order to safeguard consumers, uphold their right to privacy, and promote fair competition. While cybersecurity regulations endeavour to protect vital infrastructure and national security, regulatory frameworks like the General Data Protection Regulation(GDPR) attempt to hold businesses accountable for data breaches and privacy violations. Additionally, nations are making diplomatic attempts to set standards of behaviour and improve collaboration in cyberspace, with cybersecurity emerging as a major problem in international relations. The global landscape of cybersecurity governance and diplomacy can be shaped by punitive acts and strained diplomatic relations resulting from cyberattacks ascribed to state-sponsored actors.

Cybersecurity and the digital economy also have geopolitical ramifications that affect trade, alliances, and strategic interests. States possessing cutting-edge technology capacities have the potential to use cyber technologies for geopolitical gain and espionage, which could escalate conflicts and cause increased tensions. Because of this, cybersecurity is now a crucial component of both foreign and national security, influencing strategic planning among states and encouraging investment in cyber defence capabilities. In order to effectively combat cyber threats, foster digital innovation, and protect national interests in an interconnected world, governments must navigate these complex dynamics by striking a balance between conflicting interests and giving cooperation first priority.

CURRENT SITUATION

The Cybersecurity Tech Accord:

Adopted in 2001 by the Council of Europe, the Budapest Convention on Cybercrime is a historic international agreement designed to tackle the problems caused by cybercrime in the digital age. The first multinational treaty that focuses solely on crimes committed via the internet and other computer networks is the Council of Europe Convention on Cybercrime. Its main goals are to improve international collaboration, harmonise national legislation, and improve the capacity to successfully counter cyber threats.

Fundamentally, the Budapest Convention creates a broad framework for the definition and prosecution of cybercrime, which includes a variety of crimes such computer fraud, child pornography, hacking, and online terrorism. International cooperation in the investigation and prosecution of cyber-related offences is facilitated by the convention, which allows signatory parties to align their domestic laws and procedures by providing uniform terminology and legal standards. In order to combat new cyberthreats and protect the integrity of digital networks and systems, the convention also encourages the creation of efficient legal frameworks and investigation methods.

The Budapest Convention's facilitation of extradition and mutual legal assistance among member states is one of its main features. Through this system, nations can ask for help in locating electronic evidence, looking into cybercrimes, and bringing international offenders to justice. In order to improve cooperation and information sharing in the fight against cyber threats, the treaty also promotes the creation of specialised law enforcement units and global networks. The Budapest Convention intends to strengthen the global response to cybercrime and create a safer and more secure cyberspace for people, businesses, and governments everywhere by encouraging cooperation and capacity-building efforts.

OBJECTIVES OF THE COMMITTEE

The G20 group has several goals, including improving and developing the rules and policies that control the digital economy. With the globe becoming more interconnected and digital technology playing a major role in supporting both economic activity and societal functions, the G20 understands how important it is to create an environment that encourages creativity, development, and inclusivity. In order to achieve this, the committee works to improve upon current frameworks and create new ones that are specific to the opportunities and difficulties that the digital age presents.

The pursuit of strong cybersecurity measures to protect digital infrastructure, data, and systems from emerging threats is central to the committee's mandate. For the digital economy to remain resilient, trustworthy, and honest, cybersecurity is essential. As a result, the G20 committee works to prevent cyberattacks by encouraging global collaboration, knowledge exchange, and member state capacity building. The committee's goal is to future-proof cybersecurity policies and strengthen defences against cyberattacks by identifying upcoming risks and vulnerabilities. This will help to promote stability and confidence in the digital sphere.

GLOSSARY

- **Digital Economy:** An economy that is based on digital technologies, including the production, distribution, and consumption of goods and services that are delivered primarily through digital channels such as the internet and mobile networks.

- **Cybersecurity:** The practice of protecting computer systems, networks, and data from unauthorized access, cyber attacks, and other digital threats. It encompasses various technologies, processes, and practices aimed at safeguarding digital assets and ensuring the confidentiality, integrity, and availability of information.

- **Data Privacy:** The protection of personal information and the right of individuals to control the collection, use, and disclosure of their data. It involves policies, regulations, and technologies designed to safeguard sensitive information from unauthorized access or misuse.

- **Encryption:** The process of converting data into a format that is unreadable or indecipherable to unauthorized users, known as ciphertext, using encryption algorithms and cryptographic keys. Encryption helps secure data transmission and storage, ensuring confidentiality and privacy.

- **Malware:** Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems, networks, and data. Examples include viruses, worms, Trojans, ransomware, and spyware.

- **Internet of Things (IoT):** The network of interconnected devices, sensors, and objects embedded with internet connectivity and communication capabilities. IoT devices collect and exchange data to enable automation, monitoring, and control of physical objects and environments, but they also introduce security risks due to their susceptibility to cyber attacks.

GUIDING QUESTIONS

1. How does your delegation tackle cybersecurity threats?
2. Has your country been involved in tech/science research towards the development of a cybersecurity program?
3. Is your country one of the countries that is part of the Budapest Convention?
4. Has your country been affected by an attempt or attack of a massive cyberattack?
5. What stance does your delegation have on the digitalization of the economy?

SUPPORTING LINKS

- *International law in cyberspace*. (n.d.). https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversa

ry-an-anthology/international-law-in-cybrspace/

- *Budapest Convention - Cybercrime - www.coe.int*. (n.d.). Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention
- World Economic Forum. (n.d.). *Strategic Intelligence | World Economic Forum*. Stategic Intelligence. https://intelligence.weforum.org/topics/a1Gb0000001SH21EAG
- *What is Cybersecurity? | IBM*. (n.d.). https://www.ibm.com/topics/cybersecurity
- *Significant Cyber Incidents | CSIS*. (n.d.). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents