Wassenaar Arrangement – Need for Reform

Mains: *GS II – Bilateral, Regional and Global Groupings and Agreements involving India and/or affecting India's interests*

Why in News?

Recently, the Azure platform of Microsoft was used by the Israeli's military to spy on the Palestinians.

What is the issue?

- **Misuse of Azure** – In August, a joint investigation by *The Guardian*, *+972 Magazine* and *Local Call* revealed the misuse of *Microsoft's Azure* to store audio recordings of Palestinians' phone calls.

  Microsoft Azure *is a global cloud computing platform that offers a vast range of services for building, deploying, and managing applications and services.*

- The military intelligence unit of Israel had built a cloud-based surveillance system using.
- **Unit 8200** – It is considered Israel's equivalent to the U.S.'s National Security Agency.
- It was reportedly uploading "audio files of millions of calls by Palestinians in the occupied territories" into a dedicated Azure environment.
- **Concerns** – Presently the modern Internet is built on vast computing backbones that a very small number of companies control it.
- But the modern infrastructure of Microsoft was used to deepen Israel's repression of Palestinians.
- It raised difficult questions about how export regimes can govern services, they may never have imagined when those rules were drafted.

What is the Wassenaar arrangement?

- **Wassenaar Arrangement** – It is a voluntary, multilateral "export control regime" for conventional arms and dual-use goods and technologies.

  Export regimes *are international agreements between supplier countries to control the export of sensitive goods and technologies to prevent the proliferation of weapons of mass destruction.*

Dual-use *refers to the ability of a good or technology to be used for multiple purposes - usually peaceful and military.*

- **Established in** – The Arrangement, formally established in July 1996.
- **Secretariat** – It is in Vienna, Austria.
- **Purpose** – To ensure that the transfer of conventional arms and dual-use items does not contribute to destabilizing military capabilities or fall into the hands of terrorists.
- **Function** – It serves as an information exchange forum where participating states provide information on arms transfers, share insights on potential proliferation risks, and report on export license denials.
- **Structure** – The Arrangement operates through a plenary meeting, where decisions are made by consensus, and a small Secretariat based in Vienna, Austria.
- **Scope** – It covers conventional arms, such as small arms and light weapons, military aircraft, and armored vehicles, as well as a wide range of dual-use goods and technologies.
- **Membership** – It includes 42 participating states, primarily from NATO and the European Union.
- **India** – Became the 42nd member in 2017.

What are the issues with wassenaar arrangement?

- **Treating export as physical transfer** – Major obstacle is that many control regimes still conceptualise 'export' as physical transfer or download.
    - **For example,** the structure of the Arrangement was however conceived in an era when control meant physical exports of devices, chips, hardware modules, etc., and software transfers were written off as incidental.
- In the cloud, an export can also be remotely executed or invoked in API calls
- **Voluntary nature of the arrangement** – The Arrangement's voluntary nature is a weakness in high-risk settings.
- **Loopholes –** Moreover, the Arrangement is based on consensus, and any member can block modifications.
- As a result, the Arrangement's coverage is patchy and many states have loopholes to allow "defensive security research" and internal technology transfers.
- **Diversity of cloud** – Cloud services are global, a user in one country can trigger concerns in another
- **Rapid expansion of technology** – Cloud and AI technology move at high velocity, and the difficult to track and align.
- **Issues with domestic laws** – Even when a technology is controlled, the Arrangement requires individual countries to implement controls as per their domestic export control legislation, which often differs in ambition and political will.

What reforms need to be done?

- **Expanding the scope** – To bring the Arrangement into operational relevance, its scope needs to expand significantly.
    - **For example**, its list of controlled technologies should explicitly include

infrastructure and services that enable large scale surveillance, profiling, discrimination, and real-time control and systems that break national boundaries (for example, regional biometric systems or cross-border data transfers linked to policing).

- Including such technologies in the control lists would require devising criteria for capacity thresholds and carving out defensive, benign uses under strict safeguards and licensing.
- **Need for binding role** – The Arrangement needs binding guidance that treats remote enablement, authorisation, and granting administration rights as equivalent to export if they provide access to a controlled technology.
- The Arrangement should also embed end-use controls more systematically.
- While classical export control is about military use or the proliferation of weapons of mass destruction, for cloud services and digital surveillance the risk is mass human rights abuses.
    - **For instance**, the license to use some technology should depend on the item's technical specs as well as on the identity of the user, the jurisdiction, the oversight regime, the legal mandate, and the risk of misuse.
- **Need for compulsory membership** – The Arrangement's voluntary nature is a weakness in high-risk settings.
- States should instead adopt a binding treaty or framework with obligations that include mandatory minimum standards for licensing, mandatory export denial in atrocity-prone jurisdictions, and supervision by peer review.
- **Need for interoperability standards** – National licensing authorities must share information and align their policy decisions.
- To this end, the Arrangement should include technical interoperability standards, a shared watchlist of flagged customers or entities, and exchange red alerts in real-time,
    - **For example**, when a cloud provider offers certain services to a blacklisted state.
- **Setting up of a powerful secretariat** – A specialised technical committee or secretariat should be set up.
- It must be empowered to propose interim updates, fast-track high priority controls, and receive inputs from independent experts.
- **Adoption of sunset clause** – The Arrangement should consider adopting a sunset mechanism that causes items to fall out of the control list unless their inclusion is renewed.
- **Domain specific control** – Given the additional challenge of global consensus, the Arrangement may also consider hosting a domain-specific control regime for AI, digital surveillance, cyber weapons, etc.
- This should align with the overall regime while possessing the ability to evolve faster.

How far these reforms be realistic?

- **Resistance from countries** – Some powerful states may resist stricter controls of cloud services by arguing it would stifle innovation, sovereignty and/or impose undue regulations on private industry.
- A small number of holdouts can still block changes to the Arrangement as it exists, especially those that benefit from providing surveillance technologies abroad.

- **Intricate tasks** - Mapping cloud systems to control categories, define thresholds, distinguishing benign versus malign use, and implementing cross-border licensing is an extremely intricate enterprise.
- **Possibility of reforms** – Some states, are already pushing national export controls on 'high technologies' currently beyond the Arrangement's reach.
    - **For example**, The EU's dual-use regulation now treats the transmission of cloud services as potentially subject to rules that apply to dual-use technologies.
- There's also leverage, as specified under the UN Guiding Principles, because cloud providers are large and interconnected.

What lies ahead?

- Stricter export controls could join corporate human rights duty frameworks and limits on public procurement to reinforce incentives on providers to refuse certain customers.
- The realities of cloud services and SaaS expose significant gaps, rendering the Arrangement incapable of being a credible shield against the misuse of cloud services.

Reference

[The Hindu| Wassenaar Arrangement]