Main submitter: The Republic of India

Co-Submitters: Turkey, Singapore, Japan, Indonesia, South Africa, Malaysia, Denmark, Italy

Signatories: South Sudan, Libya, Nigeria, Ireland, Switzerland, Iran, Slovenia, Sierra Leone, Micronesia, Sri Lanka, Iran, Samoa, Spain, Australia, Rwanda, South Korea, Mexico, The Netherlands.

Topic: Expanding regulations to mitigate the unsupervised resurgence of private military and security companies.

The General Assembly,

Recognizing the growing presence of Private Military and Security Companies (PMSCs) in international conflicts and their potential impact on national sovereignty and civilian protection,

Reaffirming the importance of upholding international humanitarian law and international human rights,

Acknowledging the important security frameworks PMSCs can offer to protect government and civilian infrastructure,

Concerned that there is no legally binding definition of private military and security companies,

Acknowledging the Montreux Document (2008) and the International Code of Conduct mechanisms governing the activities of (PMCS),

Emphasizing that the outsourcing of state security, such as direct participation in hostilities, intelligence gathering, and border enforcement, undermines state sovereignty and weakens national security institutions,

1. *Calls for* strong accountability and justice for victims, through means such as, but not limited to:
    a. A duty for PMSCs to report any use of force or serious incident to the authorities within 48 hours,
    b. Independent national investigations into every serious incident,

c. Cooperation between states to collect evidence, share information and hand over suspects across borders,
d. Access for victims to justice, in line with the victim-centred approach of the Human Rights Council, including:
    i. The right to bring a case before national courts,
    ii. Fair compensation, as well as medical and psychological support,
    iii. Protection for victims and witnesses who speak out,
e. A rule that no contract can give PMSC personnel immunity from prosecution,
f. Clear penalties for companies that break the rules, including fines, loss of licence and bans from future government contracts,
g. A yearly report from each state to the Human Rights Council's intergovernmental working group on PMSCs, reporting incidents;

2. *Requests* that the responsibilities of home states, contracting states and territorial states be made clear, through the following examples but not limited to:

a. Contracting states should:
    i. Hire only licensed companies with a proven human rights record,
    ii. Enforce rules on the use of force and the duty to respect international law,
    iii. Publish the main details of their contracts with PMSCs under a legal framework,
    iv. Remain responsible for what the company does, even after the work has been contracted out,
b. Require the consent of the state before any foreign PMSC operates on its territory,
c. Ask home states to make sure their courts can prosecute their PMSCs and employees for crimes committed abroad,

d. Demands all states to stop paying PMSCs with natural resources such as gold, oil or mining rights, and to publicly report any such deal;

3. Calls for a clear international definition of private military and security companies (PMSCs) and clear limits on their jurisdiction and capabilities, in ways such as but not limited to:

a. PMSC is a private company that provides military or security service, which includes:
    i. Armed guard and protection,
    ii. Training of armed forces and police,
    iii. Cyber security, intelligence and surveillance services,
    iv. Operation and maintenance of weapon systems;
b. List functions that are strictly the responsibility of the state and should never be out sourced to PMSCs such as:
    i. Direct combat,
    ii. Prisoner interrogation,

4. *Advises* Member States to enact and enforce comprehensive domestic legislation regulating PMSCs through:

a. Mandatory transparent licensing and registration prior to recruitment, export services, or deployment abroad,
b. Rigorous vetting processes to ensure personnel have no prior criminal records;
c. Professional training requirements for employees,
d. Disclose beneficial ownership and financial backing to prevent the use of shell corporations to obscure accountability;

5. *Urges* all Member States to require strict licensing and end-user verification for PMSCs acquiring or transferring dual-use surveillance and intrusion tools, while mandating meaningful human

control and international Humanitarian Law (IHL) compliance for any PMSC AI deployment in autonomous weapons or offensive cyber operations, with PMSC leadership, operators, and contacting states held legally liable for unmonitored operations;

6. *Condemns* payments of private military companies through the holding of natural resources such as diamonds, as diamond oil or gold, and calls on Member States to end this practice, including through:

a. develop a sophisticated monitoring system for the payment of PMCs,

b. restrictions on anonymous payment sources,

c. transparent logbooks for the payments of PMCs, that would be available on request to share with a UN Body;

7. *Encourages* the creation of independent monitoring mechanisms to:

a. Investigate allegations of human rights violations,

b. Monitor PMSC activities in conflict-affected regions,

c. Publish periodic reports on company compliance;

8. *Encourages* all Member States to engage fully in the United Nations Global Mechanism on developments in the field of ICTs in the context of international security, to prevent Private Military and Security Companies (PMSCs) from exploiting regulatory gaps in cyberspace, specifically, but not limited to:

a. Establishing a standardized, rapid-response incident reporting mechanism through national Computer Emergency Response Teams (CERTs) to document, attribute, and share intelligence on unauthorized offensive cyber operations conducted by PMSCs, utilizing frameworks such as:

i. The UN Global Intergovernmental Points of Contact (PoC),

ii. The OSCE Cyber Points of Contact Network (CBM 8),

iii. The EU CSIRTs Network,

e. Establishing regional transparency and notification protocols that require PMSCs and their contracting entities to declare cross-border cyber capabilities and defensive contracts, thereby preventing covert offensive cyber attacks, unauthorized intelligence gathering, and hybrid warfare conducted under state or corporate deniability, modeled on frameworks including but not limited to:

i. The OSCE 16 Cyber Confidence-Building Measures,

ii. The ASEAN Regional Forum (ARF) Cyber CBMs,

iii. The OAS Inter-American Cyber CBMs,

9. *Calls upon* Member States to strengthen national monitoring mechanisms for PMSCs through:

a. Establishing or improving registration and licensing systems for companies operating under their jurisdiction,

b. Designating appropriate national authorities to supervise PMSC activities,

c. Conducting regular reviews of companies' compliance with relevant national and international legal obligations;