28 June 2021

Call for submission**: **Open-ended intergovernmental working group mandated to elaborate the content of an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies

Introduction

Private Military and Security Companies (PMSCs) and their clients operate in spaces with limited transparency and accountability that are increasingly digitized. The use of PMSCs has historically been a complicated topic as there are many grey areas to take into consideration. The complex nature of their use has made it difficult for victims to seek justice for the violation of their human rights. Resolution 36/11 established the Working Group for a period of three years. The new mandate given to the Working group on PMSCs under resolution 36/11 of October 2017 was to elaborate the content of an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies, without making any presumptions about the ultimate legal nature of the potential future framework.

We respond to the call for contributions to this process with great interest. The CyberPeace Institute is an independent NGO based in Geneva, working to encourage accountability in cyberspace and to ensure the protection of human security, dignity and equity in digital ecosystems. We followed the working group's second session in April of this year and noted that many discussions touched on the use of emerging technologies and the deployment of cyber capabilities by PMSCs. Recognizing that no actor in the digital ecosystem can single-handedly address threats to human security, dignity and equity, the CyberPeace Institute supports the creation of a binding regulatory framework that can complement the existing legal and voluntary mechanisms.

This submission addresses key components that we believe should be prioritized in future discussions, in order to be a step closer to achieving our collective goal of effectively preventing human rights abuses relating to the activities of PMSCs in cyberspace and ensuring access to justice and remedies for victims of such abuses and accountability of the perpetrators.

Definitions

We draw attention to the fact that definitions of the formal structure of the business enterprise itself - Private Military and Security Company (PMSC), Private Military Company (PMC,) and Private Security Company (PSC) - remain contested and do not adequately capture the blurring of boundaries in cyberspace. We recommend focusing on the **"conduct", "services" or "activities" of PMSCs as more effective means to engage in the regulation, monitoring and oversight of potential violations.** Alongside legitimate cybersecurity services, companies may be contracted by states to deploy dual-use technologies for surveillance and tracking of vulnerable communities, as well as for providing offensive capabilities. Referring to specific conduct and services of PMSCs also allows to capture situations in which there is no transparency around the deployment of cyber capabilities by private actors in violation of human rights (e.g. via spyware and malware). We thus propose that the regulatory framework focuses on the conduct, services and activities of PMSCs in order to prevent human rights abuses and to provide victims with effective remedies, including for their actions in cyberspace.

In relation to the application of the regulatory framework in 'complex environments', we recall that digitalization has added a layer of entanglement, as many core state functions have been outsourced or privatized. **In situations of both international and non-international armed conflict, as well as in times of peace**, states are increasingly reliant on privately-controlled services, many of them of a digital nature, in areas such as immigration, border control, or surveillance. **All situations of private security conduct should be open to regulation, monitoring and oversight in the framework of this regulatory mechanism.** In cyberspace, most operations fall below the threshold of war and are made possible by complex supply chains, endangering human rights on a large scale.

Scope

A regulatory mechanism for PMSCs needs to **take into account existing technologies but also upcoming ones**. Modern technologies, ranging from drones to biometric systems, facial recognition and autonomous weapons have populated the list of technologies used in conflict and peacetime scenarios and will continue to do so as innovation develops at an exponential rate. A new legal instrument needs to be designed with the use of modern technologies in mind, as these are often operated by private security contractors. Potential governance gaps for the use of new technologies should not represent ways to circumvent human rights protections and to affect human security, dignity and equity. In a new regulatory framework, PMSC-related human rights and humanitarian law violations need to be addressed effectively by **imposing due diligence obligations that also cover cyber capabilities**. Moreover, **jurisdictional and mutual legal assistance matters for cyber operations must also be addressed.**

Accountability, transparency, remedy

The regulatory framework should be centered on improving the **accountability of both states using PMSCs and PMSCs themselves for operations that impact human rights**. Harm has an indiscriminate nature in cyberspace, due to its dual-use nature. Transparency over the type of activities engaged in is thus crucial on both state and industry sides. Lack of transparency affects the extent to which victims have meaningful access to information and to an effective remedy. We welcome the inclusion of a grievance mechanism for PMSCs misconduct that does not result in serious violations of international and human rights law or humanitarian law, as long as it does not prejudice **the right to an effective judicial remedy**. For serious abuses committed by PMSCs using digital tools, significant adverse consequences may be triggered at a societal level (e.g. affecting critical infrastructure and essential services) and in other states, requiring **adequate redress**. It is worth recalling that norms of responsible state behavior, as discussed by the OEWG on developments in the field of information and telecommunications in the context of international security and UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, form an integral part of the application of international law in cyberspace.

Inclusivity

We stress the importance of an inclusive approach to the development of the regulatory mechanism, with the **full involvement of civil society not only throughout the negotiations, but also in the implementation of the regulatory mechanism**.

We thank you again for the opportunity to express our thoughts on what topics need to be included for an international regulatory framework on the regulation, monitoring and oversight of the activities of PMSCs. We strongly believe that if a human-centric approach is used, with the goal of working towards accountability, while keeping in mind the impact of existing and emerging technology, the framework will be equipped to not only address current issues but also future ones. The CyberPeace Institute stands ready to assist in the next steps.