Inputs for the report on victims of mercenaries, mercenary related actors, and private military and security companies

Submitted by USALAMA Reforms Forum

Usalama Reforms Forum is a Kenyan based Public Safety Research and Innovation Organization founded as a Police Reforms lobby in 2008 with the mandate of consolidating civil society engagement in the security sector reforms programs in the country.

P.O. Box 49806, 00100

Nairobi, Kenya

Cell:+254 721 967 932/+254725150643

email: caleb.wanga@usalamaforum.org

website: www.usalamaforum.org

I. The background

Twice a year, the Working Group on the use of mercenaries appeals for comments to form sufficient evidence to inform thematic studies to be presented at the September session of the Human Rights Council and at the General Assembly in October. The next thematic report of the Working Group to be submitted to the Human Rights Council is on the situation of victims of mercenaries, mercenary-related actors and private military and security companies (PMCS).

Whereas human rights violations and violations of international humanitarian law by mercenaries, mercenary-related actors and private military and security companies occur in peacetime, conflict and post-conflict situations. There is little accountability and victims face obstacles to obtaining effective remedies, leading to almost total impunity for violations.

The objective of this report inputs is to tease out the current major obstacles to accountability and redress for the use of mercenaries, including new forms of cyber mercenary practices, including: secrecy and opacity of mercenaries, mercenary-related activities, and activities of PMCS, as well as lack of transparency and access to information; Complex business and corporate structures and jurisdiction-related issues; Regulatory gaps in national legislation, including criminal and civil sanctions against such actors for violations, and in particular the lack of monitoring and accountability mechanisms, threaten the victims' right to effective remedies; Regulatory gaps at the international level and failure to meet international obligations.

II. Research Scope and Key Issues

We recommends that States must take measures to prevent human rights violations, including by mercenaries, mercenary-related actors and private actors such as private military and security companies. They have an obligation to ensure that all perpetrators are investigated, prosecuted and sanctioned for violations of international humanitarian law and human rights, and that victims have access to effective remedies. Appropriate regulation, monitoring and enforcement are necessary given the general lack of accountability for human rights violations and violations committed by mercenaries, mercenary-associated actors and PRIVATE military and security companies. The necessary protection should be provided to victims of human rights violations committed by mercenaries, mercenary-related actors and PRIVATE military and security companies, especially those belonging to vulnerable groups who face increased barriers to access to justice.

This thematic comments herein specifically addresses the human rights implications of vulnerable groups, including women and girls, children, ethnic minorities, persons with disabilities, persons of low socioeconomic status, indigenous peoples, LGBT + communities, human rights and environmental defenders and humanitarian actors, migrants, etc.

This thematic research inputs, comments and recommendations are drafted in response to the call under the headings of the working Group's invitation and the core of the written questionnaire. In particular, they focus on the human rights impact of vulnerable groups, providing practical cases and illustrations where possible, as well as important recommendations from experts, and analysis of future developments in this area.

III. Human Rights Impact and Recommendations on Vulnerable Groups

Based on the situation of victims affected by activities and violations committed by mercenaries, mercenary-related actors and PRIVATE military and security companies, The types of human rights violations identified, the contexts in which they occur (e.g., extractive industries, detention, migratory environments, armed conflicts) and the specific groups thus identified are described and exemplified as follows.

1. Human Rights Impact and Recommendations on Children

1）Human Rights Impact：

Around the world, hundreds of thousands of children are associated with non-State armed groups, including foreign fighters. These boys and girls are forced to serve as combatants, servants, messengers or sex slaves or in other roles. They are associated with non-State armed groups in many different ways. Some boys and girls are abducted, trafficked or forced into conscription; some are born into non-State armed groups; some seem to join these groups voluntarily for various reasons.

Children are lured into armed groups for various interrelated reasons. Across conflicts, there is no evidence of any single motivation or cause for child association with armed groups. Socioeconomic conditions, including poverty, duress, other forms of deprivation of resources and opportunities and physical and financial insecurity, are traditionally seen as the major factors behind children’s enlistment in non-State armed groups. Some children living in conflict-affected areas become associated with these groups in order to be reunited with their family members or simply because of a lack of alternatives, especially when armed groups are in physical and economic control of the community. In

the Democratic Republic of the Congo, some girls joined armed groups to escape the constant and terrifying attacks on their villages. Others joined to escape poverty and hunger. These girls were reportedly lured to join armed groups as they believed from their peers that they could obtain money and goods from the groups. A 17-year-old Iraqi boy joined Islamic State in Iraq and the Levant (ISIL) for the purpose of receiving free medical treatment for his heart condition.

2) Recommendations:

To urge Member States to criminalize in national legislation the recruitment and use of children under the age of 18 years in armed conflict. It stresses the importance of investigating, prosecuting and sanctioning those responsible for such crimes at the national level, and providing a remedy to victims of violations committed by all persons and entities within its jurisdiction.

Job openings with PMCSs might seem attractive as a potential solution for the reintegration of former child soldiers. The re-recruitment of former child soldiers into the security industry does not help to break the cycle of violence. Owing to the nature of the industry, the work environment may trigger children's memory of the traumatic events they have experienced during their association with the armed group. Thus security-related tasks at private military and security companies should not be considered as primary options for former child soldiers. When there is no alternative solution, administrative, logistics and general supporting service posts at private military security companies could be considered as a last resort to reintegrate former child soldiers.

2. Human Rights Impact and Recommendations for the Extractive Industry

1) Human Rights Impact:

Today, the extractive industry is an important client base for private military and security companies. It is also an industry with formidable economic power and considerable political influence, albeit regularly associated with concerns over access to land and human rights abuses on local communities.

Studies have shown that the more a State is rich in natural resources, the more likely it is to be subject to long-lasting armed conflicts and civil wars. The exploitation of natural resources can therefore play a major role in conflict dynamics; for instance, non-State actors are more likely to profit from easily extractable resources, such as gemstones or gold, as their extraction does not entail sophisticated technology, important investments and specialized knowledge. By contrast, resources requiring feasibility studies, teams of experts and advanced technology, such as oil and gas, are more likely to benefit States. The link between the exploitation of natural resources and armed conflicts has been widely recognized, including by the Security Council, for example in its resolutions 1173 (1998), 1237 (1999) and 1306 (2000) and 1343 (2001) on the conflicts in Angola, Sierra Leone and Liberia, and more recently in the Central African Republic (see A/HRC/39/70). These events also led to the adoption of several national and regional laws pertaining to “conflict minerals”.

In areas characterized by weak governance and in the absence of effective State security forces, extractive companies may, however, rely on private security (in-house and private military and security companies) to secure their operations. This may also be the case when State security forces have limited capacity and are asked to concentrate on key threats to national security. In such cases, private military and security companies can be engaged to perform functions beyond the regular ones; for instance, in one country, mining companies

reinforced their private security personnel in response to a high risk of kidnappings of foreign national employees, coupled with additional security measures by State security forces. Particularly acute security threats, such as criminal piracy, trafficking cartels, guerrilla forces and expropriation efforts by corrupt government regimes, may also lead extractive companies to contract private security services.

This also points to the awareness of some extractive companies of the reputational risks associated with allegations of misconduct and abuses by security providers operating in and around their sites. In some instances, extractive companies are more inclined to rely on their own employees or contractors than on State security forces in order to maintain direct influence and control over conduct by means of company policies and regulations, contracts, training and direct reporting lines. Moreover, extractive companies are likely to carefully weigh how to engage with State security forces in contexts where these forces have been accused of committing human rights violations. The reality of managing security in complex situations therefore presents sensitive challenges to extractive companies.

Those most at risk of human rights abuses are indigenous people and communities, environmental and other human rights defenders, and artisanal miners. Across these categories, women are frequently affected. In March 2019, the Human Rights Council adopted, by consensus, resolution 40/11, in which it recognized the critical role of environmental human rights defenders and the threats they faced from State and non-State actors. The consequences of abuses on the physical and mental health of victims are, in many cases, long-standing and severe.

2）Recommendations：

Although initiatives have already been taken to raise standards and respect for human rights, they are non-binding and have made only limited progress with regard to those affected by extractive operations. First and foremost, it is incumbent upon States to fulfil their international human rights obligations by making prompt efforts to address human rights concerns arising from the relationship between the extractive industry and private security. Secondly, as an industry that wields significant economic power and represents a major client base for private military and security companies, the extractive sector has the potential to leverage its influence by insisting that private military and security companies deliver services respectful of human rights of all stakeholders affected by extractive operations, and not commit human rights abuses or facilitate human rights abuses and violations by others. Lastly, private military and security companies should adopt policies and measures to avoid operating in environments with human rights risks and to redress human rights abuses should they be committed.

3. Human Rights Impact and Recommendations in Gender Perspective

1) Human Rights Impact:

The twenty-first century trend away from States' monopoly on the use of force and towards security privatization provoked considerable reflection on its effects on the quality of security provision; oversight and accountability of private military and security companies; and the availability and accessibility of security as a public good. Less focus has been put on the gendered effects of security privatization, and the different consequences it has for women, men, girls, boys and LGBTI persons; and even less on the ways that multiple and intersecting forms of discrimination further shape how individuals

experience private security services. This is all the more surprising given that many historic allegations of abuse by private military and security companies relate to sexual violence and human trafficking.

In general, women face additional barriers in gaining access to justice. This is exacerbated in relation to corporate human rights abuses, due to, for example, discriminatory laws, gendered roles, economic marginalization, social stigma, power imbalances, religious values and cultural norms. These barriers are likely to be higher for women seeking redress for human rights abuses by private military and security companies for several reasons. Specific hurdles are created by the challenges of identifying the affiliation of perpetrators and the lack of clarity regarding the hierarchical structure under which that person operates, particularly in situations where a plurality of security providers are operating. These complexities then make it difficult to determine the appropriate remedial mechanism. Additional challenges arise in contexts where the rule of law is severely diminished and judicial mechanisms may not be accessible or well-functioning. In the event that a private military and security company is identified, its grievance mechanism may not be known, easily accessible or suitable for serious human rights abuses, especially for women.

A few private military and security companies have committed to comply with the 2010 International Code of Conduct for Private Security Service Providers, which articulates the human rights responsibilities of private security companies and sets out good governance principles and standards, based on international human rights and humanitarian law, for the responsible provision of private security services, when operating in “complex environments”. For the present report, a brief review was conducted of public documents and websites of all certified

members of the International Code of Conduct Association and several members of the Association that are not yet certified with the expectation that they would adhere to higher standards. Even in these cases, however, only very few were found to display their full policies publicly.

Where such policies were available, it was possible to find integrated provisions on equal employment opportunities, equal treatment and prohibition of discrimination, as well as commitments to training on and the prevention and reporting of gender-related crimes such as sexual and gender-based violence and human trafficking, probably because these issues are explicitly referenced in the International Code of Conduct. In contrast, specific attention to stimulate the recruitment and retention of women and LGBTI persons was not found. In this regard, formal equality or gender neutrality in policies may not be sufficient to address current levels of inequality in the sector; rather special measures, such as affirmative action, may be needed. In order to do this, an assessment is required of the participation of women and LGBTI persons, as well as the barriers to increased inclusion based on, inter alia, concerns, culture and attitude of employees and job descriptions, in order to address them through policy change.

2）Recommendations：

The International Code of Conduct Association issued guidelines for private security providers on preventing and addressing sexual exploitation and abuse that seek to help companies to comply with the provisions of the Code of Conduct on sexual exploitation and abuse, mitigate the risks, and address incidents and allegations. They outline measures to address sexual exploitation and abuse in policies and procedures; codes of conduct; recruitment, performance appraisal and

discipline; training and awareness-raising; operation design and risk assessment; agreements with partners and subcontractors; and complaints and investigation mechanisms. This practical document is welcome and needs to be expanded to include guidance on other gender issues, from prevention and response to the wider spectrum of sexual and gender-based violence, to gender equality and non-discrimination.

Stringent selection and vetting procedures, anchored in national legislation, are needed to ensure that individuals with prior records of misconduct, notably in connection with sexual and gender-based violence and other human rights violations, are not hired or rehired; and this should be applied also to subcontractors. Cross border cooperation is also crucial to ensuring effective vetting procedures. The absence of appropriate records in many settings adds an additional layer of difficulty to holding private military and security companies and their personnel accountable. Thus vetting procedures should extend to exercising due diligence to find alternative means to conduct background checks. Internal reporting systems should be established to enable reporting to the regulatory authority, as well as gender-sensitive complaint processes and whistle-blower policies.

Policies on continual training should also be a legal requirement. In such policies, private military and security companies should set out training content, recurrence and any other requirements. Training criteria and curricula provide a key opportunity to raise awareness on gender, including prohibitions of any type of discrimination, harassment, sexual and gender-based violence and human trafficking, and to train personnel at all levels and in all functions to recognize and report differentiated human rights impacts on various segments of the population.

4. Human Rights Impact and Recommendations for Border Management

1）Human Rights Impact：

The Working Group sent several communications jointly with other special procedure mandate holders. An urgent action and a joint media statement were issued highlighting allegations of human rights violations and abuses in an immigration detention center in the Americas in the context of the COVID-19 pandemic. Allegation letters were addressed to two Governments and a company regarding the alleged role of a private military company in violations of international humanitarian law and violations and abuses of international human rights law allegedly committed during the armed conflict in Sri Lanka between 1984 and 1988, as well as the related lack of accountability and remedies for victims. Allegation letters were also addressed to Governments and one non-State actor regarding the use of mercenaries and related actors in the context of hostilities near Tripoli, Libya, followed by a joint media statement.[1]

Today, immigration and border management has become a multibillion-dollar business, with global border security identified as a potential market for further growth in the coming years. The amount of outsourcing to private security has surged with migrants used to justify privatization of State security functions. Diverse corporate actors have positioned themselves to benefit from the aforementioned security approaches to migration and the corresponding hikes in public budgets for border security, with privatized border management and security now a lucrative source of contracts. While the biggest markets have traditionally been concentrated in states of destination as part of policies to stem migration, demand for such services in states of

[1] https://spcommreports.ohchr.org/

transit and/or departure is steadily growing, spurred by externalization and other measures.

In recent years, a growing number of States have contracted national or local construction and infrastructure companies to erect physical barriers in the form of walls, fences, often fitted with razor wire, and watchtowers along their land borders. Border guards are deployed at various points along these physical structures, and in some locations, private security guards are also present. In addition, guards tasked with preventing entry by land, air and sea are equipped with physical assets, such as maritime patrol vessels, drones, helicopters and airplanes, purchased from large defence companies and national, and sometimes transnational, shipbuilders. As explained below, high-tech tools are deployed in support of this physical infrastructure and equipment. These businesses have thus become de facto part of the policies of securitization of borders and criminalization of migrants.

2) Recommendations:

Under the international human rights framework, States retain their obligations when they privatize the delivery of services that may have an impact on the enjoyment of human rights, including when they contract out to the private commercial sector activities involving the use of force and the detention of persons.[2] States should protect against human rights abuses by third parties, including private companies, and take positive steps to fulfil human rights. Specifically, they must ensure that "any delegation of border management functions

[2] A/HRC/17/31, commentary to guiding principle No. 5. See also Committee on Economic, Social and Cultural Rights, general comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, para. 22; Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant, para. 8; and Cabal and Pasini Bertran v. Australia (CCPR/C/78/D/1020/2001), para. 7.2.

to private actors … does not undermine human rights", and that "private actors engaged by the State in migration governance are held accountable" for human rights abuses.[3] In so doing, States must take appropriate measures "to prevent, punish, investigate or redress the harm caused by … acts of private persons or entities".[4]

In the absence of an international legally binding instrument for the regulation, monitoring and oversight of the activities of private military and security companies, two main initiatives have been developed to raise standards within the industry: the Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict (2008); and the International Code of Conduct for Private Security Service Providers (2010). Both initiatives, however, have notable gaps in relation to the immigration and border management sector; neither document mentions this sector specifically. Additionally, the former is applicable in armed conflict situations and the latter in so-called complex environments (see the definition in sect. B of the Code). They therefore fail to capture the broad range of companies that provide security-related services for immigration and border management and the variety of contexts and environments in which they operate. These companies are thus often left unregulated.

Border security technologies and monitoring services accompany and reinforce the visible physical border infrastructure. Purchased primarily from companies specializing in information and advanced technologies, technologies such as radar and ground sensor systems, cameras equipped with night vision, electro-optical systems and high-resolution imaging are part of high-tech surveillance and detection

[3] See www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_ Guidelines.pdf, guideline 2.12; and www.ohchr.org/Documents/Issues/Migration/ PrinciplesAndGuidelines.pdf, principle 1, guideline 6.
[4] Human Rights Committee, general comment No. 31, para. 8.

systems that track regular and irregular movements, often providing real-time information on virtually all movements within an area of coverage. Dual-use items, sold as having been battlefield tested, have been put to increasing use in immigration and border management. One of the most commonly used technologies is drones, which are also employed in armed conflict. Operated by national or regional border officials or by private contractors, they have become a central tool in border surveillance operations. This has had the dangerous effect of bringing military concepts and technologies into the field of migration.

Today, an essential component of this regime is biometric data. Data gathered enables States to identify and verify or authenticate migrants based on physiological and behavioural characteristics. It is used for a variety of purposes, including in airport and other border controls, visa applications, age determination assessments, asylum procedures, refugee registration and deportation decisions. Combined with other personal and private information obtained through a myriad of sources, companies facilitate the collection and storage in databases of vast amounts of data about migrants that is then processed, analysed and exchanged. Companies have developed platforms that enable users to search across databases, allowing them to cross-reference data collected for different purposes. This push towards interoperability carries risks, for example, due to greater interactions between law enforcement and immigration databases. Among other things, immigration authorities have allegedly used this information to track, detain and deport migrants, including children.

In the absence of adequate privacy safeguards in many states, there are risks that data is gathered in a non-transparent manner and without informed consent, stored for long periods, and becomes outdated even

while the database is still in use. Decisions taken during screening processes for migrants, including refugees and asylum seekers, that rely heavily on such technology with its presumed rationality and superiority, lack nuanced human judgment and risk potentially serious errors. Given the high-tech nature of such systems, States may lack adequate legislation, knowledge and expertise to provide effective oversight of these operations. Moreover, abuses of the right to privacy generated by these systems are likely to go underreported as migrants may be unaware of their rights or unable to exercise them due to the vulnerable situations in which they find themselves.

5. Human Rights Impact and Recommendations for Humanitarian Service

1） Human Rights Impact:

The presence of private military and security companies has taken place in a context in which the humanitarian space is treated as being full of security threats that can be managed, if not mitigated, by security services. It is noted that an increased propensity for criminalization of humanitarian actions, particularly if such actions do not align with State objectives. Humanitarian actors also operate in contexts where there is growing anti-terrorism legislation. They are often required to negotiate access to populations in need with armed groups that may be defined by some as terrorist groups. This may result in humanitarian actors seeking the expertise of private military and security companies, as the presence of the latter is deemed critical for operational effectiveness, further compromising adherence to the principles of impartiality, neutrality and independence. Humanitarian actors may also be perceived as supporting actors suspected of terrorism whenever they engage in humanitarian dialogue with them. Added to this challenge is the presence of private military and security companies in

situations of armed conflict where they act as combatants.

In the overall context of securitization, the ethics of neutrality and independence that demark humanitarian action are becoming progressively blurred by the involvement of contractually-orientated private military and security companies. Meanwhile, these companies are subject to a structural context determined by (contractual) dependency, on clients in humanitarian contexts, and by competition with other security actors. Their corporate survival hinges on being accepted by others as a legitimate security actor, while their services are primarily assessed on short-term economic performance rather than on responding to the needs of civilian populations during humanitarian emergencies.

The Working Group received information about private military and security personnel being reportedly involved in human rights abuses, including enforced disappearances, summary executions, indiscriminate killings, and sexual exploitation and abuse.[5] Moreover, private military and security personnel may contribute to human rights violations committed by others as a result of services that they provide. In such instances, humanitarian actors using services of that private company may be associated with its actions and even with its other clients at a local level.[6] Moreover, where there is a failure by humanitarian organizations to exercise due diligence in the private military and security company contracting process, and to maintain oversight, they may inadvertently hire personnel with links to parties to a conflict, or to persons implicated in human rights violations. If

[5] James Pattison, The Morality of Private War: The Challenge of Private Military and Security Companies (Oxford University Press, 2014).

[6] The United Nations Office for Project Services utilized ArmorGroup to conduct demining operations in Afghanistan in 2008. ArmorGroup reportedly contacted warlords to provide guarding duties. Lou Pingeot, Dangerous Partnership: Private Military and Security Companies and the UN, Report (Global Policy Forum and Rosa Luxemburg Foundation, 2012), p. 28.

force is used by private military and security company personnel, it could undermine the principle of neutrality and give the impression that the humanitarian actors are involved in a conflict.[7] Accordingly, working with companies with dubious human rights records does cause reputational damage, create security risks, and significantly undermine operations.[8]

Numerous allegations have been made against private military and security companies for indiscriminate and excessive use of force against civilians, resulting in many civilian deaths. Such incidents have also occurred when these personnel have been engaged in humanitarian-type support services, including the guarding of convoys, personnel and premises. When armed private security personnel operate closely alongside military personnel, such as State armies or United Nations peace operations, and engage in the use of force, this can compromise the principle of distinction between civilian and military persons and objects, creating confusion about legitimate targets.

Failure to distinguish between civilian and military targets constitutes a violation of the fundamental principle of distinction at the heart of international humanitarian law. Examples involving armed private military and security companies illustrate difficulties that may arise in using them, that impact negatively on human rights. Armed private military and security personnel are at times not easily distinguishable from military actors. They may therefore be perceived as legitimate military targets. In turn, they may respond with force. On occasion, private military and security personnel have used force when not targeted. If such private military and security companies are

[7] Rob Grace, "Surmounting contemporary challenges to humanitarian-military relations", in CivilianMilitary Coordination in Humanitarian Response: Expanding the Evidence Base (Watson Institute, August 2020), pp. 4 and 37.

[8] A/HRC/48/51 - E - A/HRC/48/51 -Desktop (undocs.org)

accompanying or working with humanitarian actors, the latter will likely be associated with them. This risks humanitarian actors and their premises being perceived as legitimate military targets, drawing them into a conflict.

In an unprovoked incident in Iraq in 2007, four Blackwater private security guards indiscriminately fired on Iraqi civilians in Nisour Square. This resulted in the injuring of 17 civilians, and the killing of 14, including women and children.[9] Blackwater was hired to guard coalition buildings and employees.[10] Subsequent convictions, ranging from 30 years' to life imprisonment, of the four guards by a United States court were considered an anomaly.[11] The four were pardoned in 2020 by the then President, Donald Trump - an affront to justice.[12] More recently, Dyck Advisory Group, which was hired by the Government of Mozambique to counter violence by the Al-Shabaab insurgent group in Cabo Delgado in Northern Mozambique, has been accused of the indiscriminate killings of civilians, and of failing to distinguish between civilian and military targets.[13]

Use of indiscriminate or excessive force impinges on the right to life. The loss of the life of another person in self-defence is dictated by the principle of proportionality, and it must be the only means possible of preserving one's own life. In a number of the abovementioned incidents, the use of force against civilian personnel was not proportional, and, in most incidents, it was not even predicated on the right to self-defence.

---

[9] James Pattison, The Morality of Private War: The Challenge of Private Military and Security Companies.

[10] Karen A. Mingst, "Private contractors and NGOs: new issues about humanitarian standards", paper presented at the International Studies Association Convention, Honolulu, United States, March 2005, p. 8.

[11] www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/report-pmsc-humanitarian-action2021.aspx.

[12] "US pardons for Blackwater guards an "affront to justice" – UN experts", available at www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=26633&LangID=E.

[13] Amnesty International, "What I Saw is Death": War Crimes in Mozambique's Forgotten Cape (2021).

2）Recommendations：

Access to a remedy for victims of human rights and international humanitarian law abuses, or crimes by private military and security company personnel, is contingent on the existence of reporting mechanisms, the accessibility of avenues through which to pursue a case against an entity or an individual, and financial resources, among numerous other factors. In many instances, grievance mechanisms within a private military and security company will not be known; they may not exist, or may operate on an ad hoc basis.

The rights of victims of human rights abuses to an effective remedy is firmly embedded in international law. Reparation may include cessation of wrongful conduct, guarantees of non-repetition, compensation, satisfaction, or a commitment to take disciplinary or penal action against those responsible for harm done. States' obligations to protect and fulfil human rights extend to protecting against human rights abuses by third parties, including private military and security companies.[14] Failures by a State to exercise due diligence with respect to these private actors may give rise to a right to a remedy, which could in theory be pursued against a State implicated in a private actor's conduct, or where it has failed to exercise due diligence.

Accordingly, the growing diversification of their markets is alarming given that they increasingly operate in close proximity to vulnerable populations. This diversification of services renders regulation and oversight over them even more critical. It is thus necessary to critically reflect on the types of situations and spaces in which they operate, and the array of human rights and international humanitarian law violations that can and do arise. In addressing gaps in the

[14] Human Rights Committee, general comment No. 31 (2004); and Committee on the Elimination of Discrimination against Women, general recommendation No. 28 (2010).

regulatory framework governing the conduct of private military and security companies, such reflections should be taken into consideration. In particular, we should call on States to regulate, at a minimum, critical issues such as prevention of human rights and international humanitarian law abuses, the scope of permissible activities of private military and security companies, accountability, and remedies for victims of such abuses.

Robust State regulation and oversight over private military and security companies through domestic legislation is also essential. States can establish independent mechanisms to monitor companies and to ensure they are properly vetting personnel. The role of the donors, specifically States, is critical in the ongoing process of redefining the "security industry of humanitarian action". States should also create mechanisms for sanctioning non-compliance with the laws applicable to private military and security companies, including human rights standards. Increased transparency around the use of private military and security companies, and effective regulation and oversight, would place increased pressure on these private companies to ensure that both they and their personnel adhere to human rights and international humanitarian law standards, in line with the multitude of relevant guidelines and codes that have been developed to guide them over recent years. In turn, humanitarian actors have the responsibility to ensure that those they work with adhere to human rights and international humanitarian law norms by embedding such commitments explicitly in contracts with private providers.

Going forward, a multidimensional response is encouraged to the regulation of private military and security companies. Only a comprehensive approach adopted at State and international levels can effectively regulate these private companies and ensure accountability.

In the context of humanitarian action, this necessitates further assessment on the use of private military and security companies by humanitarian actors, and other actors conducting operations in humanitarian contexts, in order to develop empirical evidence for evaluating the human rights implications of such actions. States that have been active in contracting private security providers for decades should lead the way in such efforts.

There is also a need for further efforts by the private military and security industry and the humanitarian sector themselves to self-regulate. For humanitarian organizations, the Global Interagency Security Forum has, for instance, created a tool/module to assist humanitarian agencies with exercising human rights due diligence in their contracting of private military and security companies.

United Nations Member States and United Nations entities should call for, and support, independent and impartial investigations when human rights and/or international humanitarian law abuses have allegedly been perpetrated by private actors operating under a United Nations contract. Situations in which the United Nations maintains any relationship with a private military and security company, even in the absence of a contract, should be closely monitored to ensure adequate human rights investigations.

The United Nations and its Member States need to work on the development and provision of security solutions from within United Nations internal security resources, those of host states, and those of Member States deploying to peace operations. In doing so, States should reconsider restrictions on the use of their military contingents.

Where private military and security companies are hired to manage data, such as in the context of the COVID-19 pandemic and track and trace

services, the companies should ensure that the data management and systems used comply with international and domestic law, and ensure data protection and privacy. Any data gathered must be lawfully obtained, necessary, and proportionate to the public health aim. Moreover, it must be stored securely for a specified period of time, after which such data should be destroyed.

The United Nations should further break down its statistics on sexual exploitation and abuse by "contractors" to specify whether any of them fall within the private military and security company category. Other options for compiling statistics on human rights violations by private military and security sector personnel should be explored.

6. Human Rights Impact and Recommendations for Cyber Behavior

1) Human Rights Impact:

Non-State entities that are not integrated with the armed forces play a highly significant and increasingly large role in the provision of cyber services to and on behalf of States. The evolving threat of the privatization of cybersecurity attacks through a new generation of private companies referred to as so-called "cyber mercenaries" is proliferating,14 and there is an increasingly blurred line separating the private and national spheres.

Unlike conventional private military and security companies, which have typically privatized functions and capabilities which were once monopolized by the State, cybersecurity providers first emerged and flourished in the private sector. While the most advanced global militaries have developed in-house cybersecurity expertise and capabilities, even these sophisticated military operations draw heavily on private sector cybersecurity expertise. Private cybersecurity firms include long-established for-profit players and

nimble start-ups which have won market shares in a rapidly expanding market.

The right to privacy may also be compromised by monitoring and intelligence gathering. There are substantial concerns regarding cyberoperations targeting civil society and, particularly, human rights defenders and journalists in order to disrupt their activities with a view to stifling dissent and increasing a State's control over its population. Though Governments have long employed different methods to surveil and track their citizens, dissidents, political opponents and human rights defenders, the technological tools now available such as malware and spyware allow them to do so at lower cost and to broaden the geographical reach of surveillance and increase its scope and scale, thereby enabling Governments to carry out digital repression more completely than ever before.50 Certain forms of spyware are paradigmatic examples of instruments that allow targets to be monitored remotely.[15]

At present, new cyber attacks (cyber mercenaries) involve a variety of challenges such as data and privacy security, including the challenges of data sovereignty, data leakage, data monopoly and data abuse. As the international community has not yet made clear provisions on cyberspace and data sovereignty, states have strengthened the establishment and provisions of their own data sovereignty based on the needs of national interests, resulting in continuous international disputes over data sovereignty. Foreign hackers or private organizations are employed by governments of certain states to carry out technical attacks and network penetration on the networks and hosts of targeted organizations. Some governments have even hired

[15] A/HRC/41/35, para. 9; Bill Marczak and others, Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries, Citizen Lab, 18 September 2018.

high-tech companies to gain access to foreign data, and even launched attacks on other states' critical information infrastructure.

2) Recommendations:

To prevent the impact of cyber mercenaries on human rights, states should be called upon to follow the basic principles of cyber security governance. First, respect the principle of data sovereignty. Data sovereignty is an important part of national sovereignty. All states have the responsibility and right to protect important data and personal information security related to their own national security, public security, economic security and social stability, and respect other states' data sovereignty. States should not politicize cyber security issues in the name of exercising cyber sovereignty, violate international economic and trade rules and market-oriented principles, disrupt normal cooperation in cyber infrastructure and services, and impose cyber isolation on other states. They should not rely on their technological, economic and political advantages to unfairly allocate or block important network resources and endanger the security of the global supply chain. Second, we should attach equal importance to development, security and human rights. Data security is an important tool to safeguard national security, and data development is an important trend to activate economic vitality. States should uphold the principle of equal emphasis on development, security and human rights, and balance the relationship between data technological progress and digital economy development with the protection of national security, social public interests and basic human rights. Third, we should adhere to the principle of multilateralism and coordination. Based on the principle of "good-faith cooperation" enshrined in the CHARTER of the United Nations, states should establish a comprehensive data and privacy security governance system in

accordance with the concept of extensive consultation, joint contribution and shared benefits. All parties should deepen dialogue and cooperation on the basis of mutual respect, and all stakeholders should work together to build a data and privacy security governance system. Jointly build a peaceful, secure, open, cooperative and orderly cyberspace community.

The new and evolving manifestations of mercenary-related actors therefore call for urgent attention from States and other relevant stakeholders. Considerations should be taken into account to support States and other actors when developing regulation of actors in cyberspace more effectively, with a view to ensuring respect, protection and fulfilment of the right of peoples to self-determination, protecting civilians in situations of armed conflict and safeguarding the principles of non-intervention and territorial integrity. Discussions centred on any regulation should be grounded in the international legal framework pertaining to mercenaries, notwithstanding its shortcomings, and in the broader framework of international humanitarian and human rights laws.

To prevent and mitigate the negative human rights impacts caused by mercenary and mercenary-related actors and private military and security companies in cyberspace, States should refrain from recruiting, using, financing and training mercenaries and should prohibit such conduct in domestic law and effectively regulate private security companies.

States should commit to and operationalize transparency with regard to the contracting of military support services, including for cyberoperations, and make public information on the nature of services, procurement procedures, the terms of contracts and the names of

services providers in a sufficiently detailed and timely manner. They should not invoke national security concerns as a general reason to restrict access to such information; rather, limitations on access to information must meet the test of legality, necessity and proportionality, in line with the right to freedom of expression.

States must investigate, prosecute and sanction alleged violations of international humanitarian law and human rights abuses by mercenaries, mercenary-related actors and private military and security companies and provide effective remedies to victims. Investigations, prosecutions and trials must respect and guarantee the right to a fair trial and due process of law.

At the international level, States should initiate dialogue on new and evolving forms of mercenaries and, in particular, those operating in the cybersphere in all their forms, the risks they pose to international humanitarian and human rights laws and ways to address and counter them more effectively. Any such dialogue should include international and regional organizations, civil society and experts and consider existing tools and initiatives.

All states should oppose the use of cyber mercenaries to damage other states' critical infrastructure or steal important data through information technology, as well as other activities that harm other states' national security, social and public interests.

States should take measures to prevent and stop the use of the Internet to infringe on personal information, and oppose the misuse of information technology to conduct mass surveillance against other states and illegally collect the personal information of citizens of other states.

States should require its registered enterprises to strictly abide by

the laws of the country where they are located and not require its enterprises to store data generated or obtained abroad in homeland.

States should respect other states' sovereignty, jurisdiction and right to secure data management, and should not directly transfer data located in other states to enterprises and individuals without the permission of other states' laws.

If states need to obtain cross-border data for crime fighting or other law enforcement purposes, it should be resolved through judicial assistance channels or other relevant bilateral and multilateral agreements. The conclusion of bilateral agreements between states on cross-border data retrieval shall not infringe upon the judicial sovereignty and data security of a third country.

States should establish relevant laws and regulations to prohibit information technology product enterprises and service providers from setting up backdoors in products and services, illegally obtaining user data, controlling or manipulating user systems and equipment. Information technology enterprises shall not monopolize or abuse data, or seek improper benefits by taking advantage of users' dependence on products, or force users to upgrade their systems or replace them. The product supplier shall inform the partners and users of the security defects or loopholes of the product in a timely manner and propose remedial measures.