Advance Edited Version

Distr.: General
7 February 2023

Original: English

Human Rights Council
Fifty-second session
28 February–31 March 2023
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin*, **

Summary

In the present report, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, addresses the human rights challenges and consequences of the development, use and transfer of new technologies in the context of counter-terrorism and countering violent extremism. The Special Rapporteur acknowledges the capacity of new technologies to positively transform lives and enhance the full realization of human rights, equality and dignity for human beings, and the significant potential new technologies have for addressing human rights lacunae for the most marginalized and vulnerable. Regrettably, at the same time, new technologies are being misused worldwide to restrict and violate human rights.

The present report illuminates the ways in which counter-terrorism and security are frequently used to provide political and legal justifications for the adoption of high-risk and highly intrusive technologies on the basis of exceptional threats and with the promise of strictly limited application. The report demonstrates that such rationales and limitations rarely hold, and that the claim of exceptional use to respond to security crises is a chimera, when the reality is broad and wholesale use which lacks adequate human rights or rule of law restraints. Such technologies, including biometric, surveillance and drone technology, have serious negative impacts on the enjoyment of human rights across the globe. The Special Rapporteur highlights the human rights risks inherent in the development, deployment and transfer of such technologies internationally. She is also deeply concerned about the discriminatory elements built into the development and deployment of such technologies. Negative consequences include direct violations of non-derogable rights, the integrity of which is being undermined by new technologies lacking any meaningful legal

* The present report was submitted after the deadline in order to reflect recent developments.
** The annex to the present report is being circulated as received, in the language of submission only.

oversight, and impunity for both State and non-State actors whose use and transfer of such technologies involves systemic rights-violative practice. The impact on human rights across the globe is devastating, particularly the exercise of the rights to privacy, expression, association and political participation. The Special Rapporteur's key point is that abusive practices are hardwired into the counter-terrorism and countering violent extremism arena, precisely because in the absence of an agreed international definition of those phenomena, States define them to advance a variety of interests, few of which engage human rights and the rule of law. She calls for a moratorium on the use of certain technologies, including a global prohibition of lethal autonomous weapons systems. She specifically demands a cease-and-desist policy by Member States on the transfer of such technologies to States that have a demonstrated history of human rights violations, as confirmed in the resolutions of the Human Rights Council and the General Assembly and the findings of United Nations human rights treaty bodies. In alignment with the United Nations High Commissioner for Human Rights, she calls for a moratorium on the transfer of surveillance technology. She also provides a template for a global regulatory framework on the use of surveillance technologies.

I. Activities of the Special Rapporteur

1. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, presented her report on the impact of counter-terrorism on peacemaking, peacebuilding, sustaining peace and conflict prevention and resolution[1] to the General Assembly in October 2022.

2. The Special Rapporteur continues to prioritize positive and robust engagement with Member States at the national level. She concluded constructive country visits to Maldives (15–24 May 2022)[2] and to Bosnia-Herzegovina (13–20 January 2023).[3] She conducted a working-level training visit to the United Nations Multidimensional Integrated Stabilization Mission in Mali in July 2022. In March 2021, after the issuance of her follow-up report to the joint study of 2010 on global practices in relation to secret detention in the context of countering terrorism,[4] the Government of the United States of America issued a preliminary invitation to discuss a potential technical visit focusing on the detention facility at Guantanamo Bay, Cuba, the resettlement/repatriation of former detainees and the human rights of the victims and families of victims of the events of 11 September 2001. Following extensive and constructive discussions, the detention site visit was held from 6 to 10 February 2023, and the other aspects of the visit will be implemented through April 2023. An end-of-mission statement will be issued following the end of the technical visit.

3. She has maintained her commitment to active engagement with diverse civil society actors, thereby ensuring that on-the-ground experiences of counter-terrorism and security practices are fully integrated into her work. On 9 May 2022, in advance of the High-level International Conference on Human Rights, Civil Society and Counter-Terrorism, the Special Rapporteur and Spain co-hosted a civil society workshop in Malaga. Civil society representatives from 43 countries engaged in a series of consultations to produce a civil society outcome document, which will be integrated into the official conference outcome. The Special Rapporteur also launched a global study on the impact of counter-terrorism measures on civil society and civic space, with the support of Germany and Spain, and has produced a short film series documenting the impact of counter-terrorism measures on civil society actors around the globe.

4. She makes it a priority to provide States with technical assistance and views concerning counter-terrorism legislation. Since 2021, she has provided legislation or legislative development reviews to Algeria, Austria, Belarus, Brazil, China, Denmark, El Salvador, France, Haiti, Mali, the Netherlands, New Zealand, Nicaragua, Sri Lanka, Tajikistan, Thailand, Turkey, the United Kingdom of Great Britain and Northern Ireland, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe, as well as to the European Union.

5. She issued position papers on the impact of counter-terrorism sanctions on the human rights and international law obligations of States, with particular reference to the sanctions regimes under Security Council resolutions 1267 (1999) and 1988 (2011),[5] on the human rights consequences of citizenship-stripping in the context of counter-terrorism, with specific application to the situation in north-eastern Syrian Arab Republic,[6] on the human rights and rule of law implications of countering the financing of terrorism measures,[7] on the regulation

[1] A/77/345.

[2] See A/HRC/52/39/Add.1 and Add.2.

[3] See https://www.ohchr.org/en/press-releases/2023/01/bosnia-and-herzegovina-divisive-post-conflict-politics-and-failure-address.

[4] A/HCR/49/45.

[5] See https://www.ohchr.org/sites/default/files/2022-03/position-paper-unsrct-on-unsc-use-of-ct-targeted-sanctions.pdf.

[6] See https://www.ohchr.org/en/special-procedures/sr-terrorism/return-and-repatriation-foreign-fighters-and-their-families.

[7] See https://www.ohchr.org/sites/default/files/2022-06/2022-06-13-SRCT-HR-CFT-Position-Paper.pdf.

of the international trade in counter-terrorism spyware technology[8] and on the use of armed drones.[9]

6. She remains a member of the United Nations Global Counter-Terrorism Coordination Compact Task Force and is deeply committed to the "all-of-United Nations" approach to countering terrorism, with human rights mainstreamed as affirmed into the United Nations Global Counter-Terrorism Strategy. She maintains positive cooperation with the Financial Action Task Force. She has participated in three meetings of the Inter-American Committee Against Terrorism. She has given briefings to regional groups on multiple occasions in the past year, including the Organization of Islamic Cooperation, the African Union, the European Union and the Group of Latin American and Caribbean States, and joined the Counter-Terrorism Committee for its special session in Mumbai and New Delhi, India.

II. Development, use and transfer of new technologies in the context of countering terrorism and preventing and countering violent extremism

7. It is axiomatic that new technologies can provide enormously positive benefits, enabling and advancing human dignity, facilitating sustainable development and higher standards of living, bettering health care, deepening connection and communication, promoting new educational pathways and access, and making communities safer and more efficient. Those benefits, when distributed equally, transparently and without discrimination, can make technology a partner in the promotion and protection of civil, political, economic, social and cultural rights for peoples across the planet.

8. Regrettably, the potential positive human rights impact of new technologies is far from being realized. Instead, new technologies, particularly digital technologies, are transforming the ways in which human rights are impeded and violated around the world. Several special procedures mandate holders and the United Nations High Commissioner for Human Rights have addressed the intersection of digital technologies with human rights, including in advancing xenophobic and racially discriminatory treatment and exclusion.[10] Acknowledging and affirming this important prior work, in the present report the Special Rapporteur addresses the intersection of counter-terrorism and preventing and countering violent extremism with the use of new technologies. She also takes due account of the United Nations system-wide strategic approach and road map for supporting capacity development on artificial intelligence (AI).[11]

9. She draws attention to the ways in which security imperatives and counter-terrorism rationales are used to validate the development, use and transfer of new technologies, including, but not limited to, biometric technologies, AI, unmanned aerial vehicles (drones) and surveillance tools. She decries the ways in which, under the guise of preventing terrorism, new technologies have been used that, in practice, function to profoundly undermine the rights of individuals and communities. High-risk technologies have been brought in through the proverbial "back door", validated by appeals to security that in actuality weaken broader collective security and undermine the promotion and protection of human rights. Some States with egregious human rights records, many lacking basic legislative or judicial protections, have been handed carte blanche access to high-risk technologies, which have been used by those same States to crack down on legitimate dissent, human rights advocacy, including on behalf of women and children, legal representation, journalistic expression and humanitarian action.

10. The Special Rapporteur acknowledges the threat that terrorism poses to individuals, communities and societies. She is profoundly aware of the suffering that indiscriminate acts

[8] See https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

[9] See https://www.ohchr.org/en/special-procedures/sr-terrorism/activities.

[10] See A/HRC/48/76.

[11] CEB/2019/1/Add.3.

of political violence directed at civilians produces, and her commitment to the victims of terrorism and their families and communities is unwavering. She continues to press States and multilateral institutions to meaningfully address and remedy the intersectional causes of terrorism and complex violence, including armed conflict.[12]

11. She decries, however, the elevation of blinkered security thinking that has accompanied a particularly restrictive approach to countering terrorism, including within multilateral institutions. The diagnosis of the terrorism threat in national contexts, as well as within United Nations counter-terrorism bodies, suffers from a habitual lack of holistic engagement with the causalities, overlapping forms and co-relational production of violence. Policymakers opt instead for simplistic, tired tropes about the causes of violence and propose responses that simply do not work. The practice of counter-terrorism and the incomplete analysis of the causes of terrorism contribute to an unacceptable failure to adequately address terrorism and complex violence across the globe. Responses based on inadequate causal analysis and selective data have frequently exacerbated rather than reduced violence. It is into this universe that the adoption of new technologies, often sensationalized as the "fix" to the phenomenon of terrorism, which is underdefined or simply not defined at all, occurs. In the Special Rapporteur's view, the appropriateness, necessity and added value of new technologies should be subjected to heightened scrutiny before being enthusiastically and unquestioningly adopted in counter-terrorism contexts. Fundamental questions need to be asked as to whether such technologies will contribute to, or jeopardize, the protection of human rights, the rule of law and equality in a field that is increasingly defined by infringements on human dignity.

12. She highlights three particular trends that characterize the use of new technologies in counter-terrorism and preventing and countering violent extremism. The first is the leveraging of terrorism as a policy rationale to adopt high-risk technologies, with the justification of exceptionality contaminating legal and policy debates. This includes the practice of applying national security and/or counter-terrorism exemptions in legislation regulating emerging technologies. The second relates to the absence of consistent human rights analysis and practice in the development, use and transfer of new technologies. Superficial and performative referencing to human rights is a feature in this arena. The result has been the abject failure to regulate high-risk technologies, with globally adverse human rights and international rule of law consequences. The third involves the predictable and insidious move from initial exceptional use of new technologies in narrow security contexts to general use, importing and normalizing the use of these technologies in everyday life.

13. In the present report, the Special Rapporteur pays particular attention to bilateral and multilateral technology transfers in the counter-terrorism realm, highlighting the failures of States and multilateral institutions to put in place robust oversight and control systems to prevent abuse. The apparent unwillingness to regulate the practices of private entities, including multinational corporations, that violate human rights is a cause for profound concern. The report contains several specific and actionable recommendations that build on previous recommendations to implement the Guiding Principles on Business and Human Rights (including leveraging the B-Tech Project of the Office of the United Nations High Commissioner for Human Rights (OHCHR)) and augment other treaty-based and export regulation mechanisms.

14. Regrettably, the United Nations itself appears to be engaged in supporting and enabling counter-terrorism technical assistance and capacity-building in new technologies with programming that does not fully operationalize human rights due diligence obligations and appears to systematically underweigh the risks of abuse. For United Nations entities, capacity-building and technical assistance engaging high-risk technologies, including AI, biometrics and cybersecurity, in counter-terrorism contexts must be undertaken in a manner that is consistent with international human rights, refugee and humanitarian law, and the human rights due diligence policy. They should also be guided by the Secretary-General's strategy on new technologies, the stated goal of which is to define how the United Nations system will support the use of such technologies to accelerate the achievement of the 2030 Agenda for Sustainable Development and to facilitate their alignment with the values

[12] See A/77/345.

enshrined in the Charter of the United Nations, the Universal Declaration of Human Rights and the norms and standards of international law. She supports calls in the first instance for critical dialogue among technology and telecommunications companies, United Nations human rights experts and civil society, providing a robust multi-stakeholder approach to regulation. This dialogue must be fully aligned with practical regulatory action to mainstream a human rights-based approach into the development, use and transfer of new technologies. Specific recommendations to that end are made in the present report.

15. She emphasizes the accelerator role that the Security Council has played in mainstreaming and legitimizing the widespread use of new technologies into counter-terrorism through resolutions passed under Chapter VII of the Charter.[13] She concurs with the view that the Council should exercise its capacity in counter-terrorism regulation with caution, discretion and self-restraint and avoid the overreach which has defined counter-terrorism resolutions from 1373 (2001) onwards.[14] She notes recent consideration by the Counter-Terrorism Committee regarding the abuse of drones, information and communications technologies, and new online payment and fundraising methods by terrorist actors. As Chair of the Committee in this context, India promoted meaningful and extensive dialogue with multiple stakeholders and experts, including independent civil society actors. She commends the inclusive process, which resulted in the adoption of the (non-binding) Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes,[15] and encourages the incoming Chair, the United Arab Emirates, to take a similar approach and to mainstream inclusion into the regular work of the Committee. The Declaration represents progress in recognizing the relevance of human rights to the regulation of sensitive and risky technologies. Nonetheless, the Special Rapporteur is very concerned that the Declaration does not address the broader context of the abuse of armed drones by States, the misuse of measures to counter the financing of terrorism to target civil society and humanitarian actors, or the widespread abuse of surveillance technologies by States. The Security Council and the Counter-Terrorism Committee Executive Directorate should tread very cautiously and avoid taking any narrowly framed regulatory guidance forward, even as soft law. United Nations guidance on these technologies would be severely impoverished if the regulatory conversation were to be led solely or first by a counter-terrorism body, operating in a restricted frame of reference, missing the broader multisectoral and multidimensional context which is essential to regulation or guidance and is based on respect for the rule of law and compliance with the Charter. She is concerned that such guidance will conflict with or undermine legally binding progress on these issues in parallel forums or emerging from other larger multilateral processes.

16. By way of example, the Security Council, under its expansive resolution 2396 (2017) required States (under Chapter VII) to develop systems to collect biometric data in counter-terrorism contexts, creating a global mandate on high-risk biometric data collection, storage, use and transfer, with little external consultation among technical experts and other stakeholders (including affected States).[16] The phenomenon of foreign (terrorist) fighters specifically travelling from Iraq and the Syrian Arab Republic triggered this mandate. The scale of political and security concerns at the time (2014) should not be minimized, with intelligence services indicating the movement of (potentially) hundreds of fighters affiliated with designated terrorist groups. But a gargantuan global mandate to collect biometric data on every human crossing a border on the planet premised on this specific and targeted regional threat prompts fundamental questions about the proportionality of the response. To this day, accurate global data on the number of actual transits across borders by foreign (terrorist) fighters are not available, despite the fact that the phenomenon of transit is invoked to justify the enforcement of a global biometric data collection mandate and other intrusive

[13] See A/73/361.

[14] See Eric Rosand, Alistair Millar and Naureen Chowdhury Fink, “Counter-terrorism and the United Nations Security Council since 9/11: moving beyond the 2001 paradigm”, Securing the Future Initiative, September 2022.

[15] See https://www.un.org/securitycouncil/ctc/news/delhi-declaration-countering-use-new-and-emerging-technologies-terrorist-purposes-now-available

[16] See A/73/361.

security measures.[17] As a result, biometric data collection at borders, which was originally justified on the basis of terrorist threat, functions as a way of regulating migrants,[18] providing surveillance data to States, and acts as a social control mechanism. The biometric data collection requirement of resolution 2396 (2017) was distinguished by its lack of human rights and rule of law specificity and is grievous in its human rights deficits. The implementation of such biometric data collection with only superficial human rights oversight contributes to a global calamity involving the systemic misuse of counter-terrorism measures.[19] Failure to "connect the dots" between global counter-terrorism mandates and domestic security practices is a fundamental weakness in United Nations-centred security thinking which undermines broader United Nations development, governance and rule of law efforts. Concerningly, regional bodies have not stepped up sufficiently to fill gaping human rights and rule of law deficits.

17. She notes that many new technologies involve complex systems which display inherent risks for rights protection, particularly for vulnerable groups. The failure to take account of the special characteristics of high-risk systems, the systemic devaluation of discrimination and inequality risks, and the lack of human rights-based risk management approaches define the major human rights challenges in this realm. In addition, there is little political appetite for risk reduction or willingness to put in place moratoriums on the use of certain profoundly risky technologies. Instead, a laissez-faire approach to the private sector's development and use of new technologies in security contexts prevails. Fundamentally, given the lack of an internationally agreed definition of terrorism[20] and the ingrained and systematic abuse of counter-terrorism and security laws and practices at the national level, the use of new technologies in this problematic arena creates a compounded and intersectional set of human rights challenges.

A. Biometrics

18. Biometrics is the scientific discipline concerned with measurements and metrics related to biological or behavioural characteristics that are common to all human beings while also being highly representative of a person, thus allowing for the identification of individuals. Such markers may be related to a person's physiological characteristics, such as finger or palm prints, DNA and the face, iris or retina (i.e. biological biometrics). Others are linked to behavioural patterns, such as recognition based on a person's gait (behavioural biometrics or "behavioumetrics"). As biometric identity attributes are both unique to a person and stable over time, they provide a singularly useful tool for accurate and efficient identification and authentication. However, these characteristics are also what make such data particularly sensitive,[21] thus creating a need for secure systems for data storage and processing to mitigate the risk of unauthorized access.[22]

19. Biometric tools have become a standard instrument of law enforcement and administrative agencies in various contexts, including civil identification, criminal justice and border management. The Special Rapporteur recalls that, while biometric tools have been used successfully for legitimate public interest purposes, they have also been employed in

[17] See Security Council resolution 2482 (2019).

[18] The Special Rapporteur acknowledges efforts to ensure that responsible use of biometric data collection is applied at borders in respect of migrants. See International Organization for Migration, "IOM and biometrics: supporting the responsible use of biometrics", November 2018; and Katia Lindskov Jacobsen, "Biometric data flows and unintended consequences of counterterrorism", *International Review of the Red Cross*, No. 916-917 (February 2022).

[19] See A/HRC/40/52; see also communications OTH 229/2021, ISR 11/2021, IRL 3/2022 and CHN 12/2022. All communications, and replies thereto, mentioned in the present report are available from https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[20] E/CN.4/2006/98 (paras. 26–50 and 72).

[21] The International Organization for Standardization defines a biometric characteristic as a biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition (ISO/IEC 2382-37:2017(en)).

[22] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of biometric data to identify terrorists: best practice or risky business?", University of Minnesota, 2020.

connection with gross human rights violations, atrocity crimes, and oppressive and authoritarian regimes.[23]

20. The Special Rapporteur, among others, has raised concerns regarding the collection of the biometric data of vulnerable populations and persons in diverse contexts. The collection of biometric data of populations in conflict zones, including in Iraq and Afghanistan, has raised serious concerns,[24] including with respect to the transfer of biometric data collected under the rubric of countering terrorism directly into the hands of United Nations-designated terrorist groups or individuals.[25] Special procedure mandate holders and the Committee on the Elimination of Racial Discrimination have raised concerns about the use of such technologies in the Xinjiang Uyghur Autonomous Region in the context of the application by China of its Counter-Terrorism Law and its implementing measures in the region.[26] Among a slate of measures raising serious human rights concerns, reports indicate that authorities have conducted mass collection of biometric data (such as DNA samples, fingerprints, iris scans and blood types) of residents of the region. The use of biometric data in Somalia and by Israel in the Occupied Palestinian Territory has raised similar concerns.[27]

21. She highlights that the coronavirus disease (COVID-19) pandemic has accelerated biometric data collection and both further exceptionalized and normalized its use, including the deployment of biometric capacity developed for counter-terrorism and security purposes to the management of a global health pandemic that has disproportionately affected religious, ethnic and racial minorities, other vulnerable groups and those economically and socially marginalized in society.[28] The repurposing of biometric capacity developed for counter-terrorism purposes to regulate the most marginal communities during a pandemic should concern all stakeholders.

22. The increasing use—and misuse—of biometric technology in the counter-terrorism context enjoys cover from a range of Security Council resolutions. In its resolution 2396 (2017), the Council required States to "develop and implement systems to collect biometric data" in order to "responsibly and properly identify terrorists, including foreign terrorist fighters". In its resolution 2396 (2017), the Council specifically required States to develop and implement systems to collect such data, including fingerprints, photographs and facial recognition and other relevant identifying biometric data.[29]

23. This concerted policy drive towards comprehensive biometrics collection has not been undergirded by the necessary work to achieve an adequate worldwide legal and regulatory regime. Indeed, instead of leading a comprehensive effort to agree on a set of robust international rules and standards regarding biometric/identity data collection, the chief effort in the United Nations system has simply been a capacity-building programme to facilitate that collection. That programme – the United Nations Countering Terrorist Travel Programme – includes the provision of technical assistance and support to Member States in their collection of advance passenger information and passenger name record datasets from

[23] United States Holocaust Memorial Museum, "Tattoos and numbers: the system of identifying prisoners at Auschwitz", Holocaust Encyclopedia.

[24] See United States Government Accountability Office, "DOD biometrics and forensics: progress made in establishing long-term deployable capabilities, but further actions are needed", report to congressional committees GAO-17-580 (August 2017); and Electronic Privacy Information Center, "Iraqi biometric identification system" (available at https://epic.org/privacy/biometrics/iraq.html).

[25] Following the withdrawal of coalition forces from Afghanistan in August 2021, the Taliban gained access to biometric devices left by United States forces, giving them access to extensive personal biometric data.

[26] See communications CHN 18/2019 and CHN 14/2020; and CERD/C/CHN/CO/14-17, para. 40 (b).

[27] See Keren Weitzberg, "Biometrics and counter-terrorism: case study of Somalia", Privacy International, May 2021; and communication ISR 11/2021.

[28] Fionnuala Ní Aoláin, "Exceptionality: a typology of COVID-19 emergency powers", *UCLA Journal of International Law and Foreign Affairs*, vol. 26, issue 2 (2022).

[29] Some United Nations guidance has been issued on the use of biometrics in counter-terrorism, but the Special Rapporteur assesses that it requires significant revision to address the human rights and risk dimensions of widespread biometric date use by States. See https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

all air travellers internationally, supported by the United Nations goTravel software programme, which is provided by the United Nations to States as a standard tool for data collection, sharing and analysis.[30]

24. The Special Rapporteur's particular concerns regarding the Programme and the system of personal data collection it supports include: (a) the collection of data in principle, given the degree of detail that the data, particularly passenger name record data, provide about the data subjects' lives; (b) the way in which the collection, by definition and unavoidably, occurs in relation to all travelers without discrimination, raising a clear challenge to necessity and proportionality; (c) the length of the retention period, which takes the use of such data beyond being merely a check against watchlists for particular flights and renders it capable of being a long-term record of personal behaviour from which detailed knowledge can be drawn; and (d) the data-sharing across borders between agencies of different nations raises particular risks with respect to differing standards of human rights compliance internationally. The Special Rapporteur is deeply concerned about inaccurate/discriminatory algorithmic decision-making in advance passenger information and passenger name records; she underscores the impact of the use or transfer of these technologies on freedom of movement, the right to leave and the right to seek asylum; and she highlights illegitimate targeting by States to whom data are transferred and the entirely inadequate remedies that exist for breaches of human rights that occur in the context of the use of such data.[31] She notes the limited engagement of the Programme with United Nations human rights entities. She calls for an independent audit of the Programme to ensure the integrity of its practices and technology transfer in respect of human rights, data protection and the rule of law.

25. In the same vein, the Special Rapporteur has significant concerns about the role and influence of the United Kingdom-based Biometrics Institute,[32] an organization aligned with industry and Governments which promotes standards and practices but is singularly closed and inaccessible to civil society actors and human rights stakeholders.

26. She also highlights her profound concerns about biometric data-sharing, which is strongly encouraged by the international community. One striking motif of normative counter-terrorism regulation has been the increased emphasis on the cooperation between States to advance presumed convergent counter-terrorism interests.[33] Data-sharing is a black box of international law practice, with little information available on whether and what type of biometric data are exchanged, and, more practically, on the content of data-sharing agreements. Whether human rights considerations figure at all in such agreements remains largely unknown. She highlights the tension that currently exists between repeated calls by the General Assembly and the Human Rights Council for counter-terrorism cooperation among States, in instruments from the Global Counter-Terrorism Strategy to resolutions,[34] and the abject failure to specify that such cooperation must be undertaken in compliance with States' human rights obligations, including with regard to the right to privacy.

B. Drones

27. Another field which demonstrates vividly the trend of problematic and sometimes unlawful tactics and technology originally developed for exceptional and specific counter-terrorism and national security purposes being normalized and brought into regular service is that of drones. Drone technology is proliferating at a remarkable speed. The use of armed drones worldwide, both within the confines of formal armed conflicts in particular geographical locations and as part of an asserted counter-terrorism response, remains a matter

[30] See https://learn.unoct-connectandlearn.org/course/index.php?categoryid=35 and https://www.un.org/cttravel/goTravel

[31] OHCHR, "Principles and guidelines on human rights at international borders" (October 2014), p. 13.

[32] See https://www.biometricsinstitute.org/.

[33] Security Council resolution 2482 (2019), para. 15 (c), and General Assembly resolutions 75/291, para. 30, and 60/288, annex, sect. II, paras. 3–5.

[34] See General Assembly resolution 76/169 and Human Rights Council resolution 51/24.

of substantial controversy and poses an ongoing risk to civilians and a challenge to human rights protection. Drone strikes have been used both against targets in war zones during conflict and against individuals in so-called "targeted killings" outside the geographical frame of ongoing conflict. Many of these conflicts are distinct, as they are framed not as orthodox international armed conflicts, but as theatres of counter-terrorism operation and practice. The development of drone technology is inextricably linked with military capacity and lethality,[35] and drone strikes have been consistently justified in counter-terrorism terms. The use of drone operations has been roundly criticized, including by the Special Rapporteur on extrajudicial, summary or arbitrary executions and the former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[36] The Special Rapporteur joins those condemnations and disputes the legality of the extraterritorial use of lethal drones and the multiple human rights violations such targeting engages. She voices deep unease at the acceleration of the so-called "over-the-horizon" drone deployment premised on preventing terrorism. She warns against the perpetuation of conditions conducive to terrorism, where the use of force is pernicious, unaccountable, indiscriminate in practice and driven by a hubris which devalues the lives of those on the ground.[37]

28. Despite attempts over the past decade to urge States to agree, adopt and abide by consistent standards on the lawful use of armed drones, little tangible progress has been made. States have continued to deploy this technology as a means for the targeted killing of alleged terrorists overseas, both within and outside the formal confines of armed conflict. Furthermore, numerous States have begun to expand the use of armed drones within their own borders, and new technologies have been developed, including nano-drones, drones armed with non-lethal weaponry and non-incendiary lethal drones, which raise novel human rights concerns. The Special Rapporteur stresses the lack of comprehensive regulation in this innovation-driven arena, including an absolute lack of human rights protections and enforcement.

29. She recalls the work of previous mandate holders regarding the use of armed drones. In his 2013 report to the General Assembly,[38] Ben Emmerson reviewed dozens of strikes from Afghanistan to the Occupied Palestinian Territory between 2001 and 2013 and highlighted the concerning lack of transparency in the deployment of armed drones, which, in the words of the United Nations High Commissioner for Human Rights, "creates an accountability vacuum and affects the ability of victims to seek redress".[39] In his 2014 report to the Human Rights Council, Mr. Emmerson underscored an urgent and imperative need to reach a consensus among States on a range of issues to advance human rights and humanitarian law protections.[40] The Special Rapporteur reiterates the call by the Secretary-General for a global prohibition on lethal autonomous weapon systems.[41]

30. The Special Rapporteur emphasizes that the applicability of international legal standards on the lawful use of force is not an abstract question, or a question separate from the human rights assessment of lethal drone strike events. As a matter of basic principle under international human rights law, the use of lethal force to deprive a person of the right to life must be exercised in all cases in a manner that is non-arbitrary. As the Human Rights Committee observed in its general comment No. 36 (2019), the right to life is "the supreme right from which no derogation is permitted, even in situations of armed conflict or other public emergencies that threaten the life of the nation" and deprivation of life is arbitrary "if it is inconsistent with international law or domestic law". The Committee further observed that the "use of lethal force consistent with international humanitarian law and other

[35] Imperial War Museum, "A brief history of drones". Available at https://www.iwm.org.uk/history/a-brief-history-of-drones.

[36] See A/HRC/44/38, A/HRC/25/59, A/HRC/14/24/Add.6 and A/68/389.

[37] See Atef Abu Saif, *The Drone Eats With Me: A Gaza Diary* (Boston, Beacon Press, 2016).

[38] A/68/389.

[39] Ibid., para. 41.

[40] A/HRC/25/59, para. 71.

[41] See https://www.un.org/sg/en/content/sg/statement/2018-11-11/allocution-du-secrétaire-général-au-forum-de-paris-sur-la-paix.

applicable international law norms is, in general, not arbitrary", and therefore "States parties should, in general, disclose the criteria for attacking with lethal force individuals or objects whose targeting is expected to result in deprivation of life, including the legal basis for specific attacks, … the circumstances in which relevant means and methods of warfare have been used and whether less harmful alternatives were considered".[42] Where States rely upon purported justifications which do not find adequate support in international law, the result is that such actions, by definition, violate the fundamental human rights principle of non-arbitrariness. She is deeply concerned that contemporary extraterritorial use of armed drones involves arbitrary use of force under international human rights law standards.

31. In the past five years, drone technology has followed the same well-worn path from the battlefield to the home front that has been observed in policing tactics and weaponry generally. This move from justification in the context of conflict and counter-terrorism to "regular" law enforcement tracks the consistent pattern identified in the present report, whereby approaches originally justified by exceptional counter-terrorism objectives reliably become incorporated into the local, domestic and "regular" legal system. In particular, following the adoption in 2016 by the United States Federal Aviation Authority of a rule permitting deployment of drones within domestic civilian airspace,[43] the use of drones by domestic law enforcement, first in the United States and then globally, has expanded rapidly. Research establishes that more than 1,000 police departments in the United States are currently using drone technology.[44] At least 40 police forces in the United Kingdom use drones.[45] Police forces in China use drones, with the Xinjiang Public Security Bureau having partnered with the company DJI – the world's leading drone manufacturer, which commands more than 75 per cent of the drone market.[46] Police forces in Australia, and Israel, and in Africa, Europe, the Persian Gulf and the Americas are also using them.[47]

32. It is notable that in several national contexts the justification for such use tracks national security and counter-terrorism imperatives argued to be necessary to counter domestic terrorism or protect critical infrastructure from terrorist attack. The first generation of drones used domestically by law enforcement performed surveillance functions only. They were effectively roaming closed circuit television cameras in the sky. The current generation, however, is routinely equipped with enhanced features such as thermal and night-vision imaging, automatic target tracking, loudspeakers and spotlights. Drone manufacturers have developed models aimed at the police market that are fitted with non-lethal weapons. French drone manufacturers have models for sale to law enforcement which can carry up to 18 tear gas grenades.[48] A South African drone manufacturer, Desert Wolf, has developed a drone with high-capacity paintball barrels capable of firing solid pellets, paintballs or pepper spray.[49] The "sell" for such weapons is linked directly to the articulation of domestic national security risk and challenges both from within and outside the country. The Special Rapporteur reminds business enterprises that they have a responsibility to respect all internationally recognized human rights. Businesses must avoid infringing on the human rights of others and address adverse human rights impacts they create. Fundamentally, States must hold business enterprises responsible for human rights violations. Pillar II of the

[42] Human Rights Committee, general comment No. 36 (2019), paras. 2, 12 and 64.

[43] See https://www.faa.gov/newsroom/faa-doubles-blanket-altitude-many-uas-flights?newsld=85264. 4.

[44] See https://atlasofsurveillance.org/atlas.

[45] See Chris Cole and Jonathan Cole, "Benchmarking police use of drones in the UK", UK Drone Watch, 2 November 2020.

[46] See United States Department of the Treasury, "Treasury identifies eight Chinese tech firms as part of the Chinese military-industrial complex", 16 December 2021; and Blake Schmidt and Ashlee Vance, "DJI won the drone wars, and now it's paying the price", *Businessweek*, 26 March 2020.

[47] See Christof Heyns, "Human rights and the use of autonomous weapons systems (AWS) during domestic law enforcement", *Human Rights Quarterly*, vol. 38, No. 2, pp. 350–378; and Australian Federal Police, "Australia and Sri Lanka strengthen ties over aerial drone surveillance", 9 April 2021.

[48] See Christian Enemark, "Armed drones and ethical policing: risk, perception, and the tele-present officer", *Criminal Justice Ethics*, vol. 40, issue 2, pp. 124–144. See, for example. Drone Volt's Hercules 10 tear gas model (available at https://www.aeroexpo.online/prod/drone-volt/product-180237-28892.html).

[49] See Leo Kelion, "African firm is selling pepper-spray bullet firing drones', *BBC News*, 18 June 2014..

Guiding Principles on Business and Human Rights provides an authoritative blueprint for all enterprises regarding how to meet this responsibility.[50]

33. As drone technology becomes more sophisticated, it is likely that operators will shift to micro- or nano-drones, with profound human rights consequences resulting from their easier deployment and intrusion. The Black Hornet drone, developed by Prox Dynamics of Norway, is now officially used by approximately 20 military forces, including the United States Marines, the British Army and the armed forces of Australia, France, Germany, South Africa, Turkey and others. The Black Hornet drone weighs less than 20 grams, fits in one hand and flies virtually silently. Current models can be equipped with cameras for motion and still images, with a 1.6 km range. Thousands of these micro-drones have been deployed by military forces in the past five years.[51]

34. She is additionally deeply concerned about the use of drones to surveil protests. She underscores again that this is consistent with the broader trend she identifies of the short-lived exceptional use of certain technologies and their rapid reinvention as ordinary State practice. In addition to the obvious implications for privacy, freedom of assembly, freedom of expression and the right to participate in political affairs, the use of drones coupled with the coercive power of the police brings the issues of arbitrary detention, the liberty and security of the person, and the right to life into play.

35. Given that domestic drone technology is moving in the direction of armed capabilities, it is necessary to ensure that the human rights framework that goes along with operations endangering the rights of the target to security and/or to life becomes part of the standard operating procedures of law enforcement worldwide. It is necessary to learn the lessons from the negative consequences that have followed from the use of drones in counter-terrorism contexts and apply them to their potential use in domestic law enforcement settings. The first part of that framework is the obligation of law enforcement to conduct planning beforehand, rather than simply using drones as standard practice or whenever officers prefer. The obligations relating to the planning of potentially harmful operations have been emphasized in case law, such as the European Court of Human Rights case of *McCann and others v. the United Kingdom*. The Court held in that case that risks to life must be subject to "the most careful scrutiny, particularly where deliberate lethal force is used, taking into consideration not only the actions of the agents of the State who actually administer the force but also all surrounding circumstances, including such matters as the planning and control of the actions under examination".[52] The factors that need to be taken into account when planning are noted by the Human Rights Committee in paragraph 12 of its general comment No. 36, which provides that any action which entails a risk of death or serious injury "must be strictly necessary in view of the threat posed".

36. If drones are to be used in a manner which entails a risk of death or serious injury, then State law enforcement agencies must be prepared to discharge their human rights law obligation of due investigation (which is well recognized at the international level by the Human Rights Committee,[53] the Inter-American Court of Human Rights[54] and the African Commission on Human and Peoples' Rights).[55] The key features of the obligation of investigation have been set out in authoritative form in the revised version of the Minnesota Protocol on the Investigation of Potentially Unlawful Death. Those features include the following:

[50] A/HRC/48/31, para. 11.

[51] See https://www.flir.co.uk/news-center/military/flir-wins-additional-$15.4m-contract-for-black-hornet-nano-uav-systems-for-u.s.-army-soldier-borne-sensor-program/;https://www.flir.fr/news/press-releases/flir-systems-awarded-$89-million-contract-from-french-armed-forces-to-deliver-black-hornet-personal-reconnaissance-system/; and https://www.regjeringen.no/en/aktuelt/droner/id2924942/?fbclid=IwAR0-lEUzOY5c5gorr6nY0-xBcqyGfgpCzzWQxb55Xgg9OniVOkKThv1Fumw.

[52] European Court of Human Rights, *McCann and others v. the United Kingdom*, Application No. 18984/91, Judgment, 27 September 1995, para. 150.

[53] General comment No. 31, paras. 15 and 18.

[54] *Montero Aranguren et al (Detention Center of Catsia) v. Venezuela*, Ser.C, No. 150, Judgment, 5 July 2006, para. 66.

[55] General comment No. 3, paras. 2 and 15.

(a) The investigation must be prompt;

(b) The investigation must be both effective and thorough;

(c) Investigations and the persons conducting them must also be, and must be seen to be, independent of undue influence, and investigators must be impartial and must act at all times without bias;

(d) Investigations of violations must be transparent, including through openness to the scrutiny of the general public and of victims' families.

37. It is obviously a risk that drone technology used in the law enforcement context will spill over boundaries and will be taken up in other contexts and by other actors. We have already seen this in the counter-terrorism context. The proliferation of drone technology is driven by a core group of States, but they cannot be certain that they will be able to control the further dispersal of that technology. A significant concern of the Special Rapporteur is the process by which the United Nations and States collaborate and provide technical advice and capacity-building worldwide, including through the transfer of technology such as drones.[56] States can undertake technology transfers intentionally and consciously, but they can also do so through failures of due diligence which allow for accidental, opportunistic or covert transfers of technology and capabilities. States holding powerful tools are under a heavy duty to safeguard those tools and prevent them from getting into other hands. In advancing the use of such technologies in States, the United Nations is also subject to responsibilities such as the human rights due diligence policy. The record of States with respect to keeping control of drone technology leaves a lot to be desired. As the Special Rapporteur on extrajudicial, summary or arbitrary executions noted, at least 20 non-State actors have reportedly obtained armed and unarmed drone systems, including the Libyan National Army, Harakat Thahrir al-Sham, the Palestinian Islamic Jihad, Venezuelan military defectors, the Kurdistan Workers' Party (PKK), Maute Group, Jalisco New Generation Cartel, the Houthis and Da'esh.[57] States are gradually beginning to grapple with the implications of non-State or criminal groups using drones. In April 2022, the Government of the United States launched its domestic counter-unmanned aerial systems national plan aimed at responding to malicious deployment of drones by hostile domestic actors.[58]

C. Artificial intelligence in counter-terrorism

38. The Special Rapporteur acknowledges the rapid growth in the use of AI, which is changing multiple fields of social, economic, political and military action. She recognizes that AI has the properties of a general-purpose technology, meaning that it will open up wide-ranging opportunities for application. She affirms that States are increasingly integrating AI into law enforcement, national security, criminal justice and border management systems.[59]

39. At the heart of AI development and use are algorithms, and in these contexts, AI functions as a forecasting tool. In the context of counter-terrorism, AI systems use vast quantities of data, including historic, criminal justice, travel and communications, social media and health data. The technologies may be used to create profiles of people, identify places as likely sites of increased criminal or terrorist activity and flag individuals as alleged suspects and future reoffenders.[60] The use of AI has direct consequences for the individual as regards personal interface with the power of the State, including its coercive capacity. The privacy and human rights implications of this kind of data collection and predictive activity are profound for both derogable and non-derogable rights. The Special Rapporteur highlights her profound disquiet at AI assessments being used to trigger State action in counter-terrorism contexts, from searching, questioning, arrest, prosecution and administrative

[56] See A/76/261.
[57] A/HRC/44/38, para. 9.
[58] See https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.
[59] See A/HRC/48/31.
[60] Ibid., para. 23.

measures to deeper, more intrusive surveillance, when AI assessments alone should not be the basis for reasonable suspicion given its inherently probabilistic nature. She concurs with OHCHR that the opacity of AI-based decision-making poses exceptional burdens to realizing transparency and human rights accountability for its use.[61]

40. Furthermore, the Special Rapporteur is deeply concerned with the entrenched practice of States adopting legislation that exempts the use of AI for military and national security purposes from ordinary oversight regimes. She notes in this regard the exclusion contained in the proposed artificial intelligence act of the European Union and in the Council of Europe's currently confidential "zero draft" of a convention on AI, human rights, democracy and the rule of law. In the European context, she cautions strongly against a blank national security exemption in the AI act and encourages the European Union to ensure that exemptions are proportionate and consistent with existing European Union law, including the Charter of Fundamental Rights. She recommends that legislation hold agencies such as the European Union Agency for Law Enforcement Cooperation (Europol) and the European Border and Coast Guard Agency (Frontex) to Charter obligations, as their exclusion would create a realm of exceptionality that would serve as a terrible precedent regionally and globally. She stresses that AI systems developed for military or dual-use purposes should be regulated by the AI act. She maintains the position that the Council of Europe convention must include the design, development and use of AI systems for national defence within its ambit. To exclude them would effectively make the proposed convention irrelevant to the human rights concerns that are of greatest relevance in the region.

D. Surveillance

41. The Special Rapporteur is deeply concerned about the scale of human rights violations posed by the worldwide proliferation and misuse of sophisticated intrusive cybersurveillance technologies originally justified by or intended for counter-terrorism and national security purposes. She has completed a position paper for Member States on this issue entitled "Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human rights-compliant approach".[62] A summary of the recommendations in the position paper, including the necessary features of any future regulatory framework to address the global trade in spyware, is annexed to the present report. She acknowledges that these powerful and innovative technologies can provide law enforcement and military and security services with incisive investigative and monitoring tools to disrupt terrorist violence and bring perpetrators to justice.

42. The twin twenty-first-century forces of the rapid increase in the capacity and complexity of computer hardware and software combined with the substantial expansion in the funding for, and prominence of, State counter-terrorism programmes has led to the development of a wide range of sophisticated surveillance technologies either directed at, or suitable for, counter-terrorism purposes. Standard practice in respect of counter-terrorism and criminal investigation promoted by multilateral organizations such as the Council of Europe and the International Criminal Police Organization (INTERPOL) calls for routine surveillance and collection of data by means of a range of hardware and software tools for investigative analysis.[63] The capacity for such mass surveillance as the default tool for investigation has been dramatically increased by a series of converging trends in recent years: the precipitous decline in the cost of technology and data storage; the ubiquity of digital devices and connectivity; and the exponential increase in the processing power of computers.

43. The explosion of the surveillance technology industry in the twenty-first century has been due in part to the significant flows of funding into the counter-terrorism field. It has also followed from the extraordinary powers that State agencies have arrogated to themselves on

[61] See A/HRC/48/31.

[62] See https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

[63] See Council of Europe Cybercrime Programme Office, Standard operating procedures for the collection, analysis and presentation of electronic evidence, September 2019.

the purported basis that the imperatives of counter-terrorism justify ubiquitous surveillance and government intrusion as a preventative and investigative tool.[64] In keeping with the fundamental patterns of use identified in the present report, the intrusion is typically presented as targeting only certain risk groups, typically vaguely and problematically defined by reference to (often discriminatory)[65] assumptions as to perceived risk of future harm. Such risk assessments are often based on poor or scant empirical evidence and their methodologies are often weak and ill-designed for the task at hand. The lack of clarity or rigour behind those definitions leads to a tendency for counter-terrorism operations to expand beyond the initially stated boundaries.

44. Sophisticated surveillance technology developed for counter-terrorism and national security purposes has increasingly become a focus of international concern thanks to a spate of revelations demonstrating that such tools are in fact being used to spy on politicians, journalists, human rights activists, lawyers and ordinary citizens with no links to terrorism and who pose no national security threat. Intrusive covert technology for surveillance of the content of individuals' digital communications and other information, including metadata (location, duration, source and contacts) – commonly known as spyware – has proliferated internationally out of all control and poses substantial risks to the promotion and protection of human rights. Such profound challenges are illustrated by the scandal related to the use by repressive regimes of Pegasus, a surveillance software programme manufactured by the cyberintelligence company NSO Group. Such use has prompted inquiries by the European Parliament as well as litigation. [66]

45. The impact of surveillance on multiple human rights is considerable. The Special Rapporteur highlights that the right to privacy functions as a gateway right protecting and enabling many other rights and freedoms, and its protection is intimately related to the existence and advancement of a democratic society. She therefore sees the escalation in the use of secret surveillance and the collection of content information and metadata for purposes of countering terrorism, combined with the runaway development of underregulated new technologies, as a significant threat to democratic societies.

46. Responsibility for these grave problems lies not only with the private entities that develop and either knowingly provide such technologies directly to rights-violating regimes or fail to exercise due diligence about the end use of their product, but also with State agencies that misuse these technologies in violation of international and domestic law and with States and international organizations that either actively facilitate or, through lack of robust regulation, have failed to prevent the trade of such technologies into the wrong hands.

47. While in previous eras spycraft and surveillance technology tended to be the exclusive preserve of government agencies and in-house technical experts, in the modern era the vast majority of surveillance tools used by State agencies are obtained from the private sector. Private cybersecurity firms responsible for tools with such capabilities include the Israel-based NSO, Quadream and Candiru/Saito Tech; the United Kingdom-based Gamma International; the Germany-based Vilicius Holding and Trovicor; the France-based Qosmos and Amesys; the Italy-based Area SpA and Hacking Team/Memento Labs; the firm Cytrox, which has divisions in Hungary, Israel and North Macedonia; the United States firms CyberPoint, Narus (a Boeing subsidiary), Blue Coat Systems and Cisco Systems; and the United Arab Emirates firm DarkMatter. It is a matter of urgency that the activities of these businesses and multinational corporations be regulated, in line with the obligations of States with respect to the regulation of the business sector, to prevent human rights violations.

48. In the light of recent revelations, a growing number of voices in the international human rights community have supported the call for a more robust, human rights-compliant

[64] A/69/397, para. 19.

[65] A/HRC/43/46, paras. 28–34.

[66] In March 2022, the European Parliament set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (see https://www.europarl.europa.eu/committees/en/pega/home/highlights). With regard to litigation, see United States Federal Case No. 19-cv-07123-PJH *WhatsApp Inc. et al v. NSO Group Technologies Ltd et al*.

regulatory framework for the use, sale and transfer of surveillance technology—and, in the meantime, a moratorium on the trade and transfer of such technology. The United Nations High Commissioner for Human Rights has called for a better, human rights-based system to regulate the spyware trade, including mechanisms for fixing responsibility for human rights breaches on private spyware producers by "requir[ing] by law that the companies involved meet their human rights responsibilities, are much more transparent in relation to the design and use of their products and put in place more effective accountability measures".[67] In the meantime, the High Commissioner has also called for a suspension of the trade in surveillance technology to allow States to work on an export and control regime, as well as to boost legal frameworks securing privacy.[68] Similarly, the Special Rapporteur on the right to freedom of opinion and expression, the Special Rapporteur on the situation of human rights defenders, the Special Rapporteur on the rights to freedom of peaceful assembly and of association, and members of the Working Group on business and human rights made the following joint statement:

> In recent years we have repeatedly raised the alarm about the danger that surveillance technology poses to human rights. Once again, we urge the international community to develop a robust regulatory framework to prevent, mitigate and redress the negative human rights impact of surveillance technology and, pending that, to adopt a moratorium on its sale and transfer.[69]

Support for an interim moratorium was recently repeated by OHCHR in its 2022 report on the right to privacy in the digital age.[70] In April 2022, Costa Rica became the first State to join the call for a moratorium on the trade in spyware technology,[71] while a broad coalition of civil society reiterated the demand for a moratorium at the World Economic Forum meeting, held in Davos, Switzerland, in May 2022.[72]

49. Considering the profound concerns about these technologies and the cover provided to them by contemporary discourse on and practices of counter-terrorism, the Special Rapporteur agrees with calls for the suspension of transfers of such technology. She does not rule out that States may come to the view that a permanent ban on spyware is justified, but heeds the High Commissioner's call to investigate and work towards a human rights-compliant regulatory system for the sale, use and transfer of spyware technology, either as a precursor to such a ban or as a means to ensure protection for human rights without the necessity for one. The position paper of the Special Rapporteur provides a robust new proposal for international regulation of the trade in spyware so as to minimize human rights risks.

50. Finally, she highlights the necessity of independent oversight for surveillance and data collection premised on national security or counter-terrorism grounds.[73] Noting that intelligence agencies are driving and adapting technological change and deploying an avalanche of new technologies, including machine learning, for automated offensive and defence computer network operations, the Special Rapporteur calls for substantial State investment in intelligence oversight capacity. Austerity in surveillance oversight cannot be justified given the evolution of surveillance technology, as the legitimacy of executive conduct depends on effective, modern and comprehensive intelligence oversight.[74] She urges that, as a general practice, oversight bodies be given direct access to the operational systems

[67] See https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner.

[68] See https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E.

[69] See https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[70] A/HRC/51/17, para. 19.

[71] See https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/.

[72] See https://www.accessnow.org/spyware-davos-press-conference/.

[73] A/HRC/10/3, paras. 25–78 and A/HRC/14/46.

[74] See Kilian Vieth and Thorsten Wetzling, "Data-driven intelligence oversight: recommendations for a system update", Stiftung Neue Verantwortung, 2019, p. 9.

of intelligence services[75] and that they be allowed to monitor stored data for filer errors. They should also be involved in data minimization verifications. This will ensure oversight of intelligence audit trails and create methods to enable oversight if systematic pattern identification shows high overlap with illegal and inappropriate intelligence database use. Finally, she stresses that it is urgent that a human rights-compliant review of intelligence cooperation be undertaken, [76] which will require consistent screening of transferred intelligence by methods such as data-sharing alerts to oversight bodies, consistent review of log files, deletion monitoring and a moratorium on intelligence-sharing with comparator agencies that have been identified as engaged in a consistent pattern of human rights violations.[77]

E. Effects of terrorism: victims

51. In its resolution 42/18, the Human Rights Council invited the Special Rapporteur to reflect on the negative effects of terrorism. She was pleased to provide an analysis of the legal parameters of the effects of terrorism through a human rights framework in her 2021 report to the Council.[78] In that report, she provided a comprehensive update on the human rights obligations of States to victims of terrorism, urging States to adopt a human rights approach and undertake human rights-compliant and non-discriminatory protection, investigation, remedy, participation and memorialization measures for victims of terrorism.[79]

52. She takes the opportunity to address two additional matters: the unique needs and rights of children who are victims of terrorism and the need for States to adopt human rights-compliant legislation to protect the human rights of victims of terrorism.

53. She underscores the enduring effects of terrorism on the lives of children and emphasizes the obligations of States to use the Convention on the Rights of the Child as their guide in addressing the rights of child victims. She stresses that responses to child victims of terrorism must be premised on the best interest of the child. She notes that child-centred and gender-informed trauma measures for child victims are essential and underdeveloped in many States. There must be a focus on resilience, but also on the right to child-appropriate psychological health care and education, as the pathways that enable and sustain long-term recovery for children.

54. She expresses concern about child victims of Da'esh in Iraq and the Syrian Arab Republic, thousands of whom are arbitrarily detained in Al-Hawl and Rawj camps in northern Syrian Arab Republic. She stresses that children detained in those camps must be treated primarily as victims of terrorism, consistent with the Convention on the Rights of the Child, Security Council resolution 2427 (2018) and General Assembly resolution 60/1. Every conceivable legal right to live a dignified and protected life as a child has been denied to those children. She is particularly alarmed about the situation of young boys and adolescents being detained on the premise of "association" in so-called rehabilitation facilities, in conditions which she finds meet the threshold for torture and inhuman and degrading treatment under international law. She unequivocally holds that States cannot pick and choose their preferred victims of terrorism, and to deny children so brutally treated by a designated terrorist group the protection of victims, undermines the equality principle fundamental to the protection of all victims of terrorism without discrimination. She underscores that to protect these victims from the effects of terrorism and the ongoing brutality of indefinite and arbitrary detention, human rights-compliant repatriation must be urgently undertaken.

[75] This is essential to carrying out random checks, unannounced inspections and (semi-)automated controls of intelligence agencies' data handling.

[76] She highlights as a core human rights challenge the fact that once intelligence agencies share data with foreign partners, they lose control over its subsequent use.

[77] She notes good practice by the intelligence oversight bodies of Denmark and Sweden.

[78] A/HRC/46/36, paras. 32–38.

[79] See Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (the Paris Principles); and UNSCR 1314 (2000).

55. The Special Rapporteur finally turns to the issue of domestic regulation of terrorism. She commends the model legislative provisions to support the needs and protect the rights of victims of terrorism co-produced by the Inter-Parliamentary Union, the United Nations Office on Drugs and Crime and the Office of Counter-Terrorism to which she was pleased to provide technical assistance and input.[80] She urges States to adopt human rights-compliant domestic legislation to fully and equally protect the rights of all victims, including victims of terrorism.

III. Recommendations

A. States

56. **The Special Rapporteur recommends that States:**

(a) **Pass comprehensive domestic legislation protecting individual rights and group rights in the collection of data premised on national security, counter-terrorism, violent extremism or extremism grounds;**

(b) **Ensure that, in their policies and procedures for the use of armed drones, both within and outside counter-terrorism and conflict settings, including when acting extraterritorially, they strictly observe established rules of international law, international humanitarian law and international human rights law (as applicable), and the use of armed drones in the domestic context should be subject to robust oversight mechanisms in full compliance with human rights law, with such oversight applying on a technology-neutral basis to all developments in drone technology;**

(c) **Pass comprehensive domestic legislation which adequately protects the right to privacy as a gateway right enabling and sustaining the protection of other fundamental human rights, including non-derogable rights. This includes comprehensive data protection legislation;**

(d) **Establish and support adequately resourced and independent oversight of new technologies in counter-terrorism and security contexts. This includes the establishment of independent data privacy oversight bodies. In parallel, States must ensure that intelligence oversight bodies are adequately resourced and technologically proficient to address the expansive use of technology by intelligence entities. This includes direct access to intelligence services' operational systems, access to stored data, oversight of intelligence audit trails, as well as the establishment of mechanisms of oversight for intelligence cooperation, as set out in the present report;**

(e) **Put in place moratoriums on human rights-deficient transborder cooperation that facilitates the transfer of high-risk technologies to States with poor to chronic records of human rights violations;**

(f) **Provide adequate and accessible remedies to individuals whose personal information has been mishandled or misused in counter-terrorism or preventing and countering violent extremism contexts;**

(g) **Take practical legislative steps to protect against human rights abuses by businesses in the technology sector;**

(h) **Commit to independent oversight over the United Nations Global Counter-Terrorism Coordination Compact Task Force and the Office of Counter-Terrorism.**

57. **The Special Rapporteur also calls for:**

(a) **The revision of the proposed legislation of the European Union on AI to remove national security exclusions;**

[80] See https://www.unodc.org/documents/terrorism/Website2021/220204_model_legislative_provisions.pdf.

(b) **A more transparent, inclusive and open process for the development of the Council of Europe "zero draft" of a convention on AI;**

(c) **In concurrence with the report of the High Commissioner, the adoption by States of robust export control regimes for the cross-border trade of surveillance technologies in order to prevent the sale of such technologies when there is a risk that they could be used in violating human rights, including by targeting human rights defenders or journalists;**[81]

(d) **A moratorium on the use of remote biometric recognition technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards and the absence of significant accuracy issues and discriminatory impacts and until all the recommendations set out in paragraph 53 (j) of the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,**[82] **are implemented.**[83]

B. United Nations-specific recommendations

58. **The Special Rapporteur recommends that:**

(a) **All United Nations entities, the Office of Counter-Terrorism and the Counter-Terrorism Committee Executive Directorate in particular, fully and practically address the human rights implications of providing capacity-building and technical assistance capacity in the new technology realm, including AI, biometrics and border management tools, to States with demonstrated records of human rights violations in the security and counter-terrorism arena. Both moratorium and suspension protocols on capacity-building and technical assistance in the use of high-risk technologies should be established in line with the principles and supporting frameworks of the human rights due diligence policy;**

(b) **All United Nations entities engaged in programming in these areas establish dedicated risk matrices, due diligence protocols and evaluation capacities that are timely, responsive and committed to ensuring the principle of doing no harm. The high-risk nature of these technologies and the high levels of engagement of actors outside of the definition of State security forces in the human rights due diligence policy make doing so critical;**

(c) **The Secretary-General initiate the process of internal inspection and evaluation or an external independent audit of the Countering Terrorist Travel Programme to ensure the integrity of its practices and technology transfers in respect of human rights, data protection and the rule of law.**

C. Business enterprises

59. **The Special Rapporteur emphasizes that:**

(a) **Business enterprises in new technology sectors must practically and publicly implement their operations guided by respect for international human rights law and act with due diligence so as to avoid adverse impacts on individuals and communities, including through the "respect, protect, remedy" framework set up under the Guiding Principles on Business and Human Rights;**[84]

(b) **Business enterprises in new technology must conduct comprehensive human rights due diligence. This includes conducting risk assessments of actual and**

[81] A/HRC/41/35, para. 49, and A/HRC/44/24, para. 40. In those reports, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the High Commissioner called for a moratorium on granting export licences for surveillance technologies.

[82] A/HRC/44/24.

[83] A/HRC/48/31, para. 59 (d).

[84] See https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

potential human rights impacts, both direct and indirect, during all phases of business operations;

(c) **Businesses enterprises engaged in the development, use and transfer of high-risk new technologies must be subject to more stringent regulation and oversight by legislatures, courts and international regulation, including significant financial and administrative penalties for a failure to adopt adequate due diligence practices.**

Annex

Draft Proposed State Commitments with Respect to the International Trade in Spyware

1. The current response to the challenge posed to human rights by the extremely powerful tools of the contemporary spyware industry is fractured and inadequate. Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles on Business and Human Rights, the effectiveness of which is undermined by the absence of a binding enforcement arm. Domestic private law doctrines form an inconsistent patchwork, with ample room for argument about degrees of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with. They also necessitate victims of unlawful surveillance having the knowledge and the means to use litigation to hold private companies to account. At the same time the export control system was developed for the radically different context of conventional arms. It grants exporting States generous latitude in their decision-making, providing the conditions for confusion, inconsistency, and arbitrage between jurisdictions.

2. All of this means that there is no obvious mechanism for accountability if corporations fail to advert to the harms to which their spyware technology may cause or contribute, and no clear deterrent to prevent producers from developing and trading in such technology without concern for its potential impacts.

3. As a result, the way forward for regulation of the spyware trade requires a novel approach which avoids the gaps in the existing patchwork of purported oversight and accountability methods.

4. A human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes;, and, in any event, (c) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed. Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.

5. It is therefore recommended that States adopt commitments substantively equivalent to the following draft proposals:

> *'Each State party shall, within two years from the date of their signature, give binding domestic effect to the following obligations (whether through the enaction of domestic legislation or such other steps (if any) as are required under its national law):*

1. Companies domiciled within their jurisdiction are prohibited from manufacturing or offering for sale or other provision spyware technology which fails to display the following cumulative characteristics:

(a) Not automatically granting access to all data and/or metadata once the spyware infiltrates a network, computer, or device, and instead providing that the user must positively select the types of data and/or metadata for monitoring;

(b) Not automatically granting access to any data and/or metadata regarding contacts of the target network, computer, or device, and instead providing that the user must positively select any contacts for monitoring;

(c) Providing in all cases of use of the spyware that there is created an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were affected. This record must include a record of the producer and customer for the spyware technology, so that judicial authorities may properly be able to identify the producer and purchase of spyware used in any particular instance;

2. Companies domiciled within their jurisdiction are made subject to a binding obligation to undertake a human rights due diligence exercise upon the purchasers, and, if different, the reasonably foreseeable end users, of spyware technology sold. Such human rights due diligence shall be proportionate to the risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

3. As a separate and independent obligation, companies domiciled within their jurisdiction are made subject to a binding obligation only to sell spyware technology in circumstances where they can prove that there is no tangible risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

4. For the avoidance of doubt, while the fact that such companies have obtained guarantees or assurances of compliance with international human rights law from purchasers, and/or, if different, the reasonably foreseeable end users, may be taken into account in the due diligence exercise and in the companies' assessment of the real risk of breach, the mere fact of such guarantees or assurances will not, of itself, be sufficient to demonstrate compliance with their obligations set out above;

5. As a separate and independent obligation, companies domiciled within their jurisdiction are subject to a binding obligation not to sell spyware to the agencies of any State which is not itself a signatory of this treaty;

6. Breaches of the obligations set out above are to be actionable in the ordinary domestic courts of the State on the application of persons including but not limited to persons capable of demonstrating that they are likely (subject to an appropriate evidential burden) to have been victims of breaches of international human rights law connected with the use of that companies' technology; and

7. In the event that a court determines that a breach has occurred, the persons bringing actions in respect of the same are entitled to such remedies as are available in domestic law adequately to compensate them for the violations of their international human rights which are found to have occurred.