Privacy International's response to the call for input to a report on human rights implications of new and emerging technologies in the military domain

November 2023

Introduction

Privacy International (PI) welcomes the opportunity to provide input to the study of the UN Human Rights Council Advisory Committee on the human rights implications of new and emerging technologies in the military domain (NTMD) to be presented to the Human Rights Council at its sixtieth session.[1]

PI[2] is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

As a way of introduction to our replies, we would like to make the following general observations:

- Firstly, the line between military tech and civilian tech is blurring.[3] Increasingly governments are relying on the very same technologies for military as well as civilian uses. It is often the case that technologies deployed in military domain finds their way in civilian contexts. The opposite is also true, particularly in relation to the development and deployment of surveillance technologies and beyond.

[1] UN Human Rights Council, 'Human rights implications of new and emerging technologies in the military domain', Call for contributions, https://www.ohchr.org/en/hr-bodies/hrc/advisory-committee/human-rights-implications
[2] 'Privacy International', https://privacyinternational.org/
[3] PI, 'Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds', 2020, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

- Secondly, many NTMD, like other existing and emerging technologies, are data driven: they rely on the processing of vast amount of data, including personal data, to operate. Hence the protection of the right to privacy, including the protection of personal data, is paramount.
- Thirdly, there is an emerging nexus of private capital and defence funding-initiatives deploying militarised and security-oriented technologies, with the development of public private partnerships which raise specific concerns related to democratic accountability and human rights.[4]

In the following sections, PI responds to some of the questions included in the questionnaire and further illustrates the above points. This submission provides an overview of the legal frameworks, human rights challenges, and potential risks associated with the design, development, deployment, and use of NTMD. It focuses primarily on the right to privacy and the data protection issues that arise in this context, highlighting key domestic regulatory gaps. It then also underscores concerns in relation to upholding the right to equality and non-discrimination in the design and use of NTMD. It further explores the role, risks, and responsibilities of private entities in the development and deployment of these technologies. A significant focus of the submission turns into PI's work that highlights the blurred lines between new technologies emerging in the military and civilian domains, with a particular emphasis on facial recognition technology (FRT), data analytics, and drones. Finally, the submission discusses the crucial role of civil society in relation to NTMD, advocating for greater transparency, accountability, and regulation.

1. Legal frameworks currently applicable to the design, development, deployment and use of new and emerging military technologies in the military domain (NTMD) and key domestic regulatory gaps

PI has long documented the use of surveillance technologies without adequate domestic legal framework despite the fact that the application of these technologies interfere with the right to privacy and other human rights. As these technologies process personal data their use must be prescribed by law and limited to that strictly and demonstrably necessary to achieve a legitimate aim. The domestic law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion with someone's privacy.

[4] PI and NT4T, 'All roads lead to Palantir', 2020, https://privacyinternational.org/report/4271/all-roads-lead-palantir

The rules of international humanitarian law (IHL) also known as the law of war or the law of armed conflict, is a set of rules that seeks, for humanitarian reasons, to limit the effects of armed conflict.[5] It protects persons who are not, or are no longer, directly or actively participating in hostilities, and imposes limits on the means and methods of warfare. IHL does not directly address NTMD as such, yet these rules continue to apply to new and emerging military technologies in the military domain (NTMD) to the extent that they are applicable and regulate some aspects of them. The rapid development of such technology and uncertainty about how it will be employed in practice makes it even more pressing to ensure that all relevant international standards are considered and applied.[6]

In addition to IHL, international human rights law (IHRL) is also applicable in this context, including the right to privacy and the protection against unlawful surveillance as interpreted by international and regional experts and courts apply in the context of an armed conflict.[7] This derives from the text of international human rights treaties and confirmed by human rights monitoring bodies and courts.[8] The right to privacy, as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, is particularly relevant when considering NTMD. This includes the protection of personal data, which is becoming increasingly important with the advancement of technology relying on the processing of vast amount of data.[9] While the right to privacy under international human rights law is not absolute, any instance of interference must be provided by law and subject to a careful and critical assessment of its necessity and proportionality.[10]

In the context of NTMD, the right to privacy becomes relevant in several ways. For example, consider the use of autonomous systems and robotics in the military domain.[11] In the development phase, these technologies are likely to amass large amounts of data; and

[5] ICRC, 'What is international humanitarian law?', Legal factsheet, 2022, https://www.icrc.org/en/document/what-international-humanitarian-law

[6] Y Shereshevsky, 'International humanitarian law-making and new military technologies' (2022) 104(920-921) *IRRC* 2131.

[7] L Doswald-Beck, *Human rights in times of conflict and terrorism*, OUP, 2011, p 5; Report to the Human Rights Council of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, 29 January 2007, A/HRC/4/20, paras 18-28; H-J Heintze, 'On the relationship between human rights law protection and international humanitarian law' (2004) 86(856) *IRRC* 789.

[8] AComHPR, *Democratic Republic of Congo v Burundi, Rwanda and Uganda*, Com 229/99, 29 May 2003; IAComHR, *Coard et al v United States*, Case 10.951, Report No 109/99, 29 September 1999; ECtHR, *Issa v Turkey*, Judgment, 16 November 2004. See also ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, para 106; ICJ, *Case concerning armed activities on the territory of the Congo (Democratic Republic of the Congo v Uganda)*, Judgment, 19 December 2005, para 216.

[9] OHCHR, 'International standards: Privacy in the digital age', https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards; PI's Guide to International Law and Surveillance, December 2021, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

[10] CCPR, General Comment No 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

[11] Stockholm International Peace Research Institute, 'Emerging military and security technologies', https://www.sipri.org/research/armament-and-disarmament/emerging-military-and-security-technologies

companies and governments may even compete over how to gain access to such data – whether using domestic databases to inform algorithms (e.g. national criminal or passport databases, telecommunications datasets), or using unlawful means to gain access to systems holding data (e.g. hacking an adversary nation's national database of facial images, or scraping social media). Then when deployed technologies often rely on the collection and processing of vast amounts of data, including potentially sensitive personal information. This could include biometric data collected by wearable devices used by soldiers, data collected by autonomous vehicles for navigation and targeting, or data collected at check points.[12]

Such data may be collected during a military operation but also in a context unrelated to a conflict. Such data collection and processing activities could potentially interfere with individuals' right to privacy, particularly if they are conducted without adequate safeguards. And they must be clear about the full extent of the processing; for instance, the collection by biometric data by devices in the field is only part of the system, as we must also consider the comparison of those biometrics with those from a database and the provenance of that database; or the identification of a mobile phone which is then tracked across a telecommunications system and the means of accessing that telecommunications system – each stage involves greater access to data and overcoming more safeguards.

Data protection standards, which form part of the obligations to respect and protect the right to privacy,[13] are key for NTMD. There is a growing body of evidence that data protection standards have become international standards. For instance, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe and the General Data Protection Regulation (GDPR) of the European Union are significant instruments in this regard.

Key standards from privacy and data protection that should be considered as applicable to NTMD include the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[14] These principles ensure that personal data is handled in a way that respects individual rights and freedoms, and they are crucial in the context of NTMD, where data processing can have significant implications.

[12] PI, 'Biometrics collection under the pretext of counter-terrorism', 2021, https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism

[13] General comment 17 'affirms that, in order to protect, respect and promote the right to privacy, personal data should only be collected for specified, explicit and legitimate purposes and must be processed lawfully, fairly and in a transparent manner.' CCPR, General Comment No 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988

[14] PI, 'Data Protection Guide', https://privacyinternational.org/data-protection-guide

In this regard, PI notes that data protection law is a necessary but not sufficient safeguard against abuse. While at least 137 countries around the world have enacted data protection legislation,[15] many of these laws do not apply to processing of data by security and intelligence agencies. And even when they do apply, they contain wide reaching exemptions for purposes such national security.[16]

International human rights bodies and regional human rights courts have established a plethora of human rights safeguards that need to be enshrined in domestic legislation regulating the use of technologies when they interfere with the right to privacy or other human rights. Of particular relevance to NTMD, human rights standards demand:

- demonstrable necessity and proportionality of the interference with the right to privacy prior to the deployment of any surveillance technology;
- prior judicial authorisation to determine whether to approve any deployment of surveillance technology and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies as well as persons with expertise in privacy and human rights;
- independent oversight;
- safeguards related to the retention, use and sharing of information (personal data) collected through the use of surveillance technologies, such as requirement of data minimisation, deletion of data, security of data stored, protection against unlawful access, and safeguards related to sharing to third parties;
- access to effective remedies, including notification of surveillance measures.[17]

See further below on the role of private companies.

2. Primary human rights challenges presented by NTMD

Firstly, PI has documented how armed and security forces around the world have deployed biometric surveillance technologies with the aim of identifying real or perceived enemies and surveill the population at large. They have done so often in the absence of the human rights safeguards mentioned above.

[15] UNCTAD, 'Data Protection and Privacy Legislation Worldwide', https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[16] For an illustration of key principles of data protection legislation, see PI, 'Data Protection Guide', https://privacyinternational.org/data-protection-guide

[17] PI's Guide to International Law and Surveillance, December 2021, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

For example, in Afghanistan and Iraq, the U.S. Department of Defense developed its biometric program in confluence with US military operations in the country. Its expansion was tightly linked to the goals of military commanders during the "War on Terror": to distinguish insurgents and terrorists from the local civilian population. The DOD's biometric programme was developed and implemented without prior assessment of its human rights impact and without the safeguards necessary to prevent its abuse. Its whereabouts and current use today remain unclear.[18] In Israel/Palestine, the Israeli government has been deploying biometrics, including cutting-edge facial recognition technology, in the name of counter-terrorism. The Israeli state routinely surveils and severely restricts Palestinians' freedom of movement using myriad technologies, including biometrics, which result in furthering the policies of systemic segregation. Since many Palestinians live under Israeli occupation, they have little control over the way their sensitive data is turned against them.[19]

Secondly, PI is concerned about the use of profiling and other automated decision making for surveillance purposes (including with the aim of predicting past or future behaviour) and its application to support the use of lethal force.[20] The UN Human Rights Council and the UN General Assembly have repeatedly raised concerns about the negative impact and potential of abuses of the right to privacy and other human rights related the profiling, automated decision-making, machine learning and biometric technologies. [21] For example, many commercially available facial recognition systems have been found to have different error rates, depending on people's race, and gender.[22]

These technologies rely on probabilistic reasoning, and as such, inevitably produce varying levels of false positive and false negatives. That the automated processing of metadata is used to target individuals has been known for sometimes.[23] Most recently, reports have also emerged of the Israeli army using artificial intelligence to help determine the targets for strikes

[18] PI, 'Biometrics and counter-terrorism: Case study of Iraq and Afghanistan', 2021, https://privacyinternational.org/report/4529/biometrics-and-counter-terrorism-case-study-iraq-and-afghanistan

[19] PI, 'Biometrics and counter-terrorism: Case study of Israel/Palestine, 2021, https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israelpalestine

[20] 'Privacy International's submission for the UN High Commissioner for Human Rights' report on the right to privacy and artificial intelligence', June 2021, https://privacyinternational.org/advocacy/4538/privacy-internationals-submission-un-report-right-privacy-and-artificial-intelligence

[21] See for references: PI's Guide to International Law and Surveillance, December 2021, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

[22] In his 2019 report, the UN Special Rapporteur on the right to freedom expression noted that facial recognition technology 'seeks to capture and detect the facial characteristics of a person, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics, which are often the basis for unlawful discrimination'. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35, 28 May 2019), para 12.

[23] See statement by General Michael Hayden in 2014, available here: https://www.youtube.com/watch?v=kV2HDM86XgI , and some of the related scenarios, J Naughton, 'Death by drone strike, dished out by algorithm', *The Guardian*, 21 February 2016, https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan

in Gaza.[24] The devastating consequences of application of these technologies in the context of armed conflict or more broadly the use of lethal force by state authorities raise concerns both for international human rights law and IHL.

3. Upholding the right to equality and non-discrimination in the design, development, and use of NTMD

PI would like to refer to the General Recommendation No 36 (2020) by the UN Committee against Racial Discrimination. In particular, the Committee recommends that 'before procuring or deploying such [algorithmic profiling] systems States should adopt appropriate legislative, administrative and other measures to determine the purpose of their use and to regulate as accurately as possible the parameters and guarantees that prevent breaches of human rights'.[25]

It further notes that 'when the results of an assessment of a technology indicate a high risk of discrimination or other human rights violations, States should take measures to avoid the use of such a technology.' [26] The Committee also recommends that 'States should take all appropriate measures to ensure transparency in the use of algorithmic profiling systems. This includes public disclosure of the use of such systems and meaningful explanations of the ways in which the systems work, the data sets that are being used, and the measures in place to prevent or mitigate human rights harms.'[27]

In relation to transfer and trade of NTMD, export control laws can play an important role to stop the export of technologies, when there is a risk, they will be used for human rights abuses. In practice, however, export control policies are dominated by national security considerations, with human rights often playing a peripheral role: governments tend to overwhelmingly allow exports of surveillance technologies for economic and security reasons. For example, the UK has approved over 300 license applications for the export of telecommunications interception equipment in the last few years, and rejected only 30 for human rights reasons. Further, while some governments publicly report on the applications

[24] H Davies, B McKernan and D Sabbagh, 'The Gospel': how Israel uses AI to select bombing targets in Gaza', *The Guardian*, 1 December 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets
[25] General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials adopted by the UN Committee against Racial Discrimination (CERD/C/GC/36, 17 December 2020), para 58.
[26] *ibid*, para 62.
[27] *ibid*, para 61.

that they receive and approve, the vast majority of countries do not provide any such information.[28]

A significant development in this sector is the entry into force of the EU export control rules which will make human rights considerations a central consideration for export control authorities when assessing licenses and require them to publish data on their decisions to hold them account.[29] Yet it remains to be seen how this will be further implemented.

4. Potential risks associated with using NTMD and mitigation measures

Some technologies purposefully introduce new or exploit existing vulnerabilities to conduct surveillance, thereby compromising the security of digital communications and allowing third parties to exploit these vulnerabilities. For example, while identifying cyber security vulnerabilities, testing them, and sharing these results is necessary for security, government hacking for surveillance does not seek to secure systems. Instead, the government identifies vulnerabilities to exploit them to facilitate a surveillance objective. This activity may not only undermine the security of the target system but also of other systems. Ultimately it leaves those systems vulnerable to cyber security attacks by a range of actors, including hostile governments, non-state armed groups or organised criminal groups.[30]

In the context of military cyber operations, the exploitation of vulnerabilities can serve various purposes, including surveillance, defense, and offense. For instance, military forces could exploit vulnerabilities in connected technologies, such as cars, household devices and others, devices to increase their attack surface.[31] While this could potentially enhance their offensive capabilities, it also introduces risks. Just as in the case of government hacking for surveillance, this activity could undermine the security of not only the target system but also other systems, leaving them vulnerable to cyber-attacks by a range of actors.[32] Moreover, the proliferation

[28] PI, 'Taming Pegasus: A Way Forward on Surveillance Tech Proliferation', 2021, https://privacyinternational.org/news-analysis/4602/taming-pegasus-way-forward-surveillance-tech-proliferation

[29] HRW, PI and others, 'Human Rights Organisations' Response to the Adoption of the New EU Dual Use Export Control Rules', https://www.hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf

[30] PI, 'Hacking Necessary Safeguards', https://privacyinternational.org/demand/government-hacking-safeguards; PI, 'Government hacking', https://privacyinternational.org/learn/government-hacking

[31] P Renals, 'Future developments in military cyber operations and their impact on the risk of civilian harm', *Humanitarian Law and Policy*, 24 June 2021, Future developments in military cyber operations and their impact on the risk of civilian harm - Humanitarian Law & Policy Blog (icrc.org)

[32] K Mačák and E Lawson, 'Avoiding civilian harm during military cyber operations: six key takeaways', *Humanitarian Law and Policy*, 15 June 2021, https://blogs.icrc.org/law-and-policy/2021/06/15/avoiding-civilian-harm-military-cyber-operations/

of artificial intelligence (AI) and IoT devices is expected to characterize the future of military cyber operations. These technologies could introduce new vulnerabilities or exacerbate existing ones, thereby increasing the potential for exploitation. For example, AI systems could be manipulated through adversarial attacks, while IoT devices, due to their inherent security weaknesses, could be easily compromised.[33]

In light of the above considerations, PI agrees with the recommendation by human rights experts and civil society organisations to establish a moratorium on the sale and transfer of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards, given the documented grave human rights abuses committed.[34]

Similarly, governments see the expansion of end-to-end encryption (E2EE) as a threat to their ability to access private communications and have put forth a variety of proposals for how to access E2EE communications while, purportedly, retaining their security. PI research demonstrates that to date, no proposal has successfully preserved E2EE while also providing government authorities the access they seek.[35]

Additionally, because of the unpredictability of military actions, some of the NTMD may become accessible to actors, including opposing armed forces or non-state armed groups, which can use them to commit human rights violations. For example, concerns were raised that the biometrics databases and some of the security and surveillance technologies deployed or supported by the US and others in Afghanistan may be used by the Taliban, following their take-over of the country in August 2021.[36]

5. Role, risks, and responsibilities of private entities

Because of the increasing reliance by governments on surveillance technologies developed by private companies, PI believes that specific attention should be paid on the legislative framework governing public procurement and public-private partnerships (PPP.)

[33] P Renals, 'Future developments in military cyber operations and their impact on the risk of civilian harm', *Humanitarian Law and Policy*, 24 June 2021, Future developments in military cyber operations and their impact on the risk of civilian harm - Humanitarian Law & Policy Blog (icrc.org)
[34] OHCHR, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech', 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening
[35] PI, 'Securing Privacy: PI on End-to-End Encryption', 2022, https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption
[36] PI, 'Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?', 2021, https://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems

The increasing dependence on private companies for the development of new and emerging technologies is a significant trend across the world including in the modern defense landscape. Private companies, with their innovative capabilities and technological expertise, are playing a crucial role in driving advancements in military technology. They are at the forefront of research and development in areas such as artificial intelligence, cyber security, robotics, and space technology, among others. This collaboration allows the military to leverage cutting-edge technology, accelerate the pace of innovation, and maintain a competitive edge. However, this dependence also raises concerns about security, control, and the commercialization of warfare. It underscores the need for stringent regulations, robust oversight mechanisms, and ethical guidelines to ensure that the use of these technologies aligns with international law and humanitarian principles.

PI has been documenting several cases where public authorities (including police forces, but also national and local authorities) partner with private companies in order to expand their surveillance capabilities and process mass quantities of personal data (including often biometric data, such as facial images).[37] These PPPs are taking on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services.

These concerns translate into the military domain sector not only because of the dependency on private sector therein as mentioned above but also because the defense industry has always been inextricably linked with the surveillance one. Some of the biggest surveillance producers are owned by arms industry ones.[38] For example, a well know security company responsible for building mass biometric databases in West Africa is part-owned by large arms producers, including Thales, Airbus DS, and Safran.[39]

PI has identified some common concerns related to PPPs in this field:

- lack of transparency and accountability in the procurement processes;
- failure to conduct human rights due diligence assessments;

[37] PI, 'Public-Private surveillance partnerships', https://privacyinternational.org/learn/public-private-surveillance-partnerships
[38] PI, 'The Global Surveillance Industry', 2018, https://privacyinternational.org/explainer/1632/global-surveillance-industry
[39] PI, 'Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds', 2020, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

- growing dependency on technology designed and/or managed by private companies, with loss of control over the tech applications themselves (to modify, update, fix vulnerabilities, etc.); and
- over-reliance on the technical expertise of the private company and related risk of vendor lock-in.

In many cases, the private company supplies, builds, operates and maintains the technology system they deployed, with public authorities not having sufficient knowledge or effective oversight. Lack of adequate legal framework is often compounded by limited enforcement safeguards provided for in contracts, resulting in limited or no venues for redress. We assert that any private company involved in NTMD should comply with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights.

To address these issues, we have defined corresponding safeguards that we recommend for implementation by public authorities and companies who intend to enter into such partnerships. Classified between principles of Transparency, Adequate Procurement, Accountability, Legality, Necessity & Proportionality, Oversight and Redress, together they seek to uphold human rights and restore trust in the state's public functions as these increasingly get outsourced to private hands.[40]

PI further notes that human rights impact assessments of NTMD can mitigate the risks of abuse. Human rights impact assessments of NTMD should be conducted at all stages of the technology cycle: prior to the design, during the development, the testing, the deployment and regularly thereafter in order to identify the emerging human rights risks. These assessments not only enable the identification of the risks and corresponding mitigation strategies required to respond to them, but they also provide a framework for deciding whether to go ahead with a particular initiative. The outcomes of the assessment should result in redesign or cancellation if the risks outweigh the benefit.

While certain NTMD which carry significant risks for human rights (due to the technology used and/or the sector in which they are used, see above) require additional scrutiny, PI believes that at a minimum, an impact assessment should include privacy and data protection impact assessments as well as an assessment of other human rights likely affected by the technology as well as potential discriminatory effects. Such assessments should consider the necessity and proportionality of any interference with privacy or other human rights, the risks to individuals and groups, and how these risks are to be addressed and mitigated.

[40] PI, 'Safeguards for Public-Private Surveillance Partnerships', https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

The assessments should be conducted with the participation of affected individuals and groups, civil society actors and independent experts. The outcome of the assessment should be made public and should detailed the mitigation and oversight measures envisaged.

We recommend the Advisory Committee to consider at least the following recommendations in its report:

- ensure that all companies involved in NTMD carry out any activities in accordance with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights;
- ensure that human rights impact assessments are conducted prior to the approval of any development project and that they are updated throughout the project's lifecycle;
- develop clear and consistent guidelines for human rights due diligence, including the identification, prevention, and mitigation of potential adverse human rights impacts of development projects;
- increase transparency and disclosure in their activities, including project assessments and due diligence processes;
- establish clear and accessible mechanisms for affected communities to provide feedback and file complaints regarding the potential negative impacts of their projects on human rights.

6. Some examples of the blurred lines between new technologies emerging in the military and civilian domains

As described in the replies above, PI has conducted research on the use of surveillance technologies, including as deployed in military domains, such as by militaries and/or in conflict and post situations. We have consistently advocated for compliance with international human rights law in the use of NTMD and contributed to the analysis and recommendations developed by international human rights mechanisms, such as UN Special Procedures and treaty monitoring bodies. In the process, we have been observing the line between military tech and civilian tech is blurring. Increasingly governments are relying on the very same technologies for military as well as civilian uses. It is often the case that technologies deployed in military domain finds their way in civilian contexts. The opposite is also true, particularly in relation to the development and deployment of surveillance technologies and beyond. This creates both risks and opportunities. We are presenting three key examples in that regard below.

6.a. Facial recognition technology: Clearview AI

Technology developed in civilian contexts are often repurposed in military contexts, with significant human rights and due process implications. For example, Clearview AI has been offered since the start of the war in Ukraine to the Ukrainian government,[41] at first to help them identify Russian soldiers and officials, and later reportedly extended to 'detect infiltrators at checkpoints, process citizens who lost their IDs, identify and prosecute members of pro-Russia militias and Ukrainian collaborators, and even to locate more than 190 abducted Ukrainian children who were transported across the border to live with Russian families'.[42]

But Clearview's technology has been developed through mass breaches of the laws of privacy and data protection of dozens of countries around the world.[43] The practice of this company has come under some scrutiny thanks to complaints raised by civil society, including PI and several data protection authorities have found Clearview AI in breach of applicable data protection laws, and imposed fines and ordered the company to delete and stop processing data within their respective jurisdictions. Whatever "side" this technology is provided to, in a war context the consequences are unpredictable. Even the most careful safeguards we can establish in times of peace and stability, vanish when faced with the realities of war. Giving the opportunity to a private company to exploit the distress and despair of the Ukrainian peoples to rebrand their unlawful and dangerous technology is precisely what peacetime and wartime laws must guard against.

6.b. Data management and analytics: Palantir

Palantir Technologies provides a compelling example of the blurred lines between technologies used in the civilian and military domains. Initially funded by the CIA through its venture capital branch, In-Q-Tel, Palantir began as a defense-oriented company. Its data analytics tools were designed to search, aggregate, and cross-reference large data sets to develop intelligence and insights, thereby informing decision-making in the defense sector.[44]

However, Palantir's technology has since been rolled out to civilian contexts, often with the same lack of transparency and due process that characterizes its use in the defense sector. For instance, Palantir's tools have been used by US immigration authorities, where they may

[41] PI, 'The Clearview/Ukraine partnership - How surveillance companies exploit war', 2022, https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war

[42] V Bergengruen, 'Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company', Time, 14 November 2023, https://time.com/6334176/ukraine-clearview-ai-russia/

[43] PI, 'Challenge against Clearview AI in Europe', https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe

[44] 'Palantir knows everything about you', Bloomberg, 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/?leadSource=uverify%20wall

pose a real danger to people in vulnerable positions, such as at international border crossings.[45] Furthermore, Palantir has subsequently secured contracts with the National Health Service (NHS) and other critical government departments in the UK.[46]

This growing reliance by governments on the services offered by data analytics companies like Palantir underscores the increasing convergence of civilian and military technologies. They provide analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights, and thereby inform public decision-making across sectors. Yet, it also highlights the urgent need for greater transparency and accountability in the use of such technologies, given the potential human rights implications. Civil society has been faced with a complete lack of transparency and accountability with regards to the role of Palantir's data analytics in the formulation of public policy – leaving us and the public unable to understand its rationale, nor to challenge any potential underlying human rights abuses.

6.c. Drones

The use of military-grade drones in civilian contexts, such as during protests, is also an example of the blurred lines between military and civilian technology. In various countries, for instance, there have been instances where military-grade drones, originally designed for battlefield surveillance, have been deployed for domestic law enforcement purposes.[47] These drones, equipped with high-resolution cameras and other surveillance technologies, can monitor large areas and gather extensive data. However, their use in civilian contexts raises significant concerns about privacy, peaceful assembly and other civil liberties. The deployment of these drones in these contexts are often not properly regulated raising concerns about its compliance with the principles of legality, necessity and proportionality.[48]

[45] PI, 'Who supplies the data, analysis, and tech infrastructure to US immigration authorities?', 2018, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities

[46] PI, 'The Corona Contracts: Public-Private Partnerships and the Need for Transparency', 2020, https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency

[47] J Stanley, 'Protests, Aerial Surveillance, and Police Defunding', ACLU, 2020, https://www.aclu.org/news/national-security/protests-aerial-surveillance-and-police-defunding; 'Position paper of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism on the Use of Armed Drones in Counter-Terrorism Context', 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/activities/20230103-Position-Paper-Use-Armed-Drones.pdf

[48] PI, 'Restraining protest surveillance: When should surveillance of protesters become unlawful?', 2023, https://privacyinternational.org/report/5029/restraining-protest-surveillance-when-should-surveillance-protesters-become-unlawful

On the other hand, commercial drones, which are typically used for recreational or business purposes, are increasingly finding applications in the military domain. For example, in Ukraine, commercial drones have been repurposed for military use.[49] These drones, often equipped with surveillance technology, can provide valuable intelligence in conflict situations. However, their use in a military context also raises complex legal questions. International Humanitarian Law (IHL) has little to say when drones are just equipped with surveillance tech, and hence International Human Rights Law (IHRL) provides the necessary guidance on these questions. The lack of clarity regarding the rules regulating their use in a military context underscores the need for comprehensive regulations that address these challenges.

7. Civil society's role in relation to NTMD

PI has sought information, including by leveraging freedom of information legislation in different countries across the globe, including the UK and the US, on development and use of new and emerging technologies, including data management and analytics, drones, and others. Similarly, we sought to track procurement and contracts to identify links between government and surveillance/defense technologies companies.[50]

However, as noted in replies above, transparency in the decision making related to the development, acquisition and deployment of technologies, including NTMD, is often lacking and civil society organisations and independent researchers have little to no information on the use of these surveillance technologies in military domain. These constraints limit CSOs capacity to carry out their traditional functions of independent monitoring, reporting and advocating for human rights compliance in this domain.

Among the key activities that CSOs should be allowed to conduct are:

- Monitor Governments' stances on defense tech by reviewing national defence innovation policies;
- Monitor the relevant industrial sectors and track investment and investors as well as expenditures of national 'defense intelligence units';
- Monitor changes in defence procurement and intervene in procurement processes, informing oversight bodies and regulators of the risks, and requiring the deployment of safeguards as a precondition of contracting;

[49] R Angius, L Bagnoli & R Coluccini, 'Drones on the frontlines', IRPI, 2023, https://irpimedia.irpi.eu/en-drones-on-the-frontlines/; 'Combat drones: We are in a new era of warfare - here's why', BBC News, 4 February 2022.
[50] For instance, PI, 'Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds', 2020, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

- Promote action by affected stakeholders and communities including people affected by the deployment of these technologies;
- Intervene by challenging in courts and before regulatory/oversight bodies the use of surveillance technologies when they affect the enjoyment of human rights; and
- Assist in raising media scrutiny about NTMD.