NINE

Autonomous Weapon Systems

Accountability Gaps and Racial Oppression

THOMPSON CHENGETA

The problem of impunity—the lack of accountability—when gross human rights violations by states, nonstate entities, and individuals go unpunished and victims are left without remedy is a serious threat to the human rights system. Given the foundational idea that those who violate human rights must be held responsible and that victims have a right to remedy, various national, regional, and international mechanisms have been created to ensure such accountability in times of both war and peace.

Nevertheless, some perpetrators of gross human rights violations still go unpunished and victims are left without remedies. In recent years, particularly, in countries like the United States, there has often been a concerning lack of accountability in law enforcement or the unlawful use of force against people of color. In the context of counterterrorism, there is a similar lack of accountability for the disproportionate use of force in Muslim communities, for example, in the killing of hundreds of civilians in drone strikes. Against this backdrop, states are currently developing autonomous weapon systems (AWS) whose potential use in both these areas may aggravate the problem.

This chapter examines the challenge presented by the AWS accountability gap from a racial justice perspective. It argues that any discussion of the use of such weapons must be contextualized, acknowledging first that, like many

technologies powered by artificial intelligence (AI), AWS are not neutral; they are racialized and as such can easily become tools of racial oppression.

AWS—also known as killer robots—are robotic weapons that, once activated, are able to "decide" whom to target, harm, or kill without any further human intervention or control.[1] But if machines, computers, or robots have this decision-making capability, it may be impossible to establish responsibility for unlawful acts they commit. First, since there is no human control after activation, AWS are unpredictable and may act in a manner that was not anticipated or intended by the person who activated them.[2] In the event of AWS violating international human rights law (IHRL) or international humanitarian law (IHL), it may therefore be impossible to establish the mens rea (that is, intentionality) of the person who activated them, thereby affecting the important notion of individual responsibility.[3] Second, AWS may be used in an untraceable manner that may make it impossible to hold states and nonstate entities accountable.[4] This is the accountability gap challenge, which can have an adverse effect on the right to remedy. However, it is not the only concern that is raised by AWS, which have far-reaching consequences for fundamental human rights such as the right to life, physical security, dignity, and nondiscrimination.

In the context of racial justice, this chapter focuses on the impact of AWS on the right to nondiscrimination and the right to remedy. The right to nondiscrimination is a norm of customary international law and a norm of jus cogens (from which no derogation is allowed). Discrimination on grounds of race, nationality, religion, region, or indeed any other grounds violates human dignity and is therefore internationally prohibited. The right to nondiscrimination on the grounds of race is provided for in the International Convention on the Elimination of All Forms of Racial Discrimination (CERD),[5] as well as in the International Covenant on Civil and Political Rights[6] and other regional human rights treaties.[7] CERD also provides that in cases where there has been a violation of the right to nondiscrimination—including where state agents use violent force in violation of this right—victims are entitled to a remedy, including prosecution of the offender.[8] If the current discussions on AWS continue without sufficient regard to their potential negative impact on racial justice, the consequences for the fundamental rights of Muslims, people of color, and other ethnic minorities will be far-reaching. Indeed, in the Preamble of CERD, it is noted that racial oppression is not favorable for stable geopolitics because discrimination is "capable of disturbing peace and security among peoples and the harmony of persons living side by side."[9]

Furthermore, scholars have already begun to note the link between geopolitics and emerging AI technologies such as AWS. More importantly, some have cautioned that "the relentless pursuit of AI militarization does not protect us" as "proliferating military artificial intelligence will leave the world less safe."[10] Rather, it has been strongly recommended that states should "stop the emerging AI cold war" and "focus on ethics and global cooperation."[11] To this, one would add that the weaponization of AI creates an even more precarious situation for people of color and civilians in the Muslim world who are already on the receiving end of unlawful violence. Yet, although these groups have been disproportionately affected by the use of lethal force in law enforcement and counterterrorism operations, the current United Nations (UN) discussions on AWS have not sufficiently considered the implications for racial oppression.[12] The AWS accountability gap challenge has only been discussed in general terms without specifying likely victims.[13]

Drawing on legal, ethical, and sociological theories, the following sections discuss the impact of AWS use on responsibility, accountability, and racial justice specifically in relation to the violation of fundamental human rights of people of color and civilians in the Muslim world.

Background on UN Discussions on AWS

The UN discussions on AWS have been ongoing since 2013, when the UN Special Rapporteur on extrajudicial executions (UN Special Rapporteur) submitted his annual report to the UN Human Rights Council (UNHRC).[14] At this point, AWS were yet to be deployed, and their use may have seemed a distant prospect, but in June 2021, a UN report indicated that they were deployed in Libya, noting:

> Logistics convoys and retreating HAF [Haftar-affiliated forces] were subsequently hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems such as the STM Kargu-2 and other loitering munitions. The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true "fire, forget and find" capability.[15]

The UN Special Rapporteur further noted that the development and deployment of AWS posed challenges to IHL and IHRL, and that they might violate fundamental human rights such as the right to life and human dignity.[16]

Along the same lines, UN Secretary General António Guterres` described AWS as one of the four major threats to world peace and security, saying they

were "morally repugnant, politically unacceptable and should be banned by international law."[17] Nevertheless some states[18] and scholars have argued that AWS will perform better than humans and that consequently their development and use may ameliorate the suffering of civilians on the battlefield and elsewhere where force is used.[19]

In view of the seriousness of the challenges raised by AWS, in 2014 the UN established a Group of Governmental Experts (UNGGE) on Lethal Autonomous Weapon Systems (LAWS), whose mandate is to formulate appropriate recommendations on how states should respond to AWS technology.[20] In 2021, the International Committee of the Red Cross (ICRC), an organization that is internationally regarded as the guardian of IHL, noted that states needed to adopt new laws to govern AWS.[21]

For the past eight years, the UNGGE has been involved in intensive multidisciplinary discussions on AWS, examining the issue from various standpoints, including gender perspectives. Between 2014 and 2019, it produced six reports.[22] While the concern that the use of AWS may perpetuate and/or exacerbate racial oppression has been raised by some delegates, and while it is clear that racial socialization influences their development,[23] not once were the words racism, racial oppression, racial bias, or racial discrimination mentioned in any of these six reports between 2014 to 2019—despite the fact that the 2013 UN Special Rapporteur's report highlights that AWS may be used in law enforcement situations where people of color are disproportionately affected. Furthermore, research has already shown that existing racial prejudice and bias may end up being programmed into AWS, either intentionally or unintentionally.[24]

Understanding AWS as Racialized Technology

From a racial justice perspective, any discussion of the problem of the AWS accountability gap—particularly accountability for violation of the right to nondiscrimination—and any formulation of policy on emerging related AI technologies is incomplete without acknowledging the racial identity of both perpetrators and victims. Indeed, in fighting for racial justice for victims of police brutality and unlawful killings of Black people in the United States, activists started a hashtag #saytheirnames.[25] They state that, just as the U.S. government vowed "never to forget" the victims of the September 11 terrorist attacks, they will "never forget the lives lost to the terror of racism, excessive force and countless injustices" and "never forget the Black lives taken unjustly."[26]

In all the intensive discussions about AWS' potential to violate human rights and create this accountability gap, the identities of the potential perpetrators

and victims are rarely specified. The argument is that the nonspecification of the likely victims of AI technologies like AWS is neither accidental nor inconsequential—it unfortunately functions to further white supremacy and racial oppression. Racial justice practitioners have long noted that although white supremacy has shaped a system of geopolitics and global domination, influencing white moral theory and moral psychology for hundreds of years, it remains an unnamed political system.[27] The AWS technology can be located right at the center of the politics of white supremacy and domination if one considers where AWS are currently being developed, the identity of those who are developing AWS, and the people and regions where AWS are likely to be deployed. Unlike other political systems such as socialism, capitalism, or fascism, which are openly named, studied, and critiqued, "White supremacy's power is drawn from its invisibility, the taken-for-granted aspects that underwrite all other political and social contracts."[28] It is for these reasons that in the current AWS discussions, the associated racial politics is "invisible," regardless of its presence. Charles Mills has argued that despite its being ignored in many important discussions, the Racial Contract of white supremacy exists[29] and functions to create global policies and geopolitics that favor white interests at the expense of those of other peoples.[30]

Further, the nonspecification of the potential perpetrators and victims also stems from the current mistaken approach of stakeholders to AWS technology as if it were neutral. It is important to examine the issue through the lens of social and cultural theories such as decolonial theory[31] and critical race theories. These aim to dig beneath the surface to uncover and challenge power structures that shape not only our society and geopolitics but our technological inventions, including AWS. Indeed, science has been instrumental in creating systems that are oppressive to certain peoples, reproducing social structures of authority, hierarchies of race, and oppressive geopolitics. Thus it is crucial to understand that AWS and other AI technologies are neither a simple matter of algorithms nor a mere case of great human imagination in pursuit of science; rather, such technologies are shaped by specific political and ideological projects of the powerful that permeate geopolitics as we know it today.[32] As such, adopting a noncontextual and ahistorical approach when discussing AI technologies such as AWS is a dangerous pitfall. Who's developing what, and where will it be deployed and against whom? What has been the historical experience on use of force through emerging technologies such as armed drones? Where have they been deployed? It is essential for stakeholders to address these questions. Failure to do so will result in an incomplete discussion

about rights that will be violated or victims who will be deprived of the right to remedy when AWS are used. Say their names. Acknowledge the identity of the potential or likely victims.

Studies have already noted that racialized AI military technologies will lead to algorithmic coloniality, algorithmic oppression, exploitation, and dispossession of those who have been historically oppressed.[33] It is therefore important to emphasize the social context of AWS and confront what amounts to epistemic forgeries, where AI technologies such as AWS are presented as if they are neutral technologies, free from social context. On the contrary, such technologies "come from a rather specific, White, and privileged place. They are racialised, gendered, and classed models of the self."[34]

The power of AI whiteness and the associated racial oppression is often concealed by a myth of color-blindness on such technologies. This purported color-blindness is particularly prevalent in Silicon Valley's tech-culture, where it "serves to inhibit serious interrogation of racial framing."[35] In his 2020 report and comments on emerging technologies, the UN Special Rapporteur on contemporary forms of racism noted that "States must reject a 'colour-blind' approach to governance and regulation of emerging technologies, one that ignores the specific marginalization of racial and ethnic minorities and conceptualizes problems and solutions relating to such technologies without accounting for their likely effects on these groups."[36] In the interest of racial justice, states and other stakeholders must therefore adopt approaches from critical theory to strip the cloak of invisibility from any AI whiteness associated with AWS development and deployment.[37] Thus, when discussing how AWS may violate rights and create an accountability gap, the identity not only of the likely victims but also of the perpetrators must be clearly acknowledged.

Contextualizing the Use of AWS and the Accountability Gap Problem

In the ongoing discussions on AWS, many stakeholders have approached the technology as if these were typical conventional weapons that will basically be used in armed conflict. Indeed, part of the UNGGE's eleven Guiding Principles is that the UN Convention on Conventional Weapons (UNCCW) is the appropriate forum for AWS discussions.[38] But by definition the mandate of the UNCCW is restricted to conventional weapons of war.[39] As such, the potential use of AWS in the context of law enforcement and counterterrorism operations outside armed conflict is ordinarily excluded from its discussions. Yet such use

is highly likely.[40] With these concerns in mind, the scenario in Box 1, originally presented by the author at a workshop titled "Malign Uses of Artificial Intelligence/Autonomous Weapon Systems" organized by the UN Institute for Disarmament Research, may provide an instructive hypothetical case study.

Box 1: Malign Uses of Artificial Intelligence/Autonomous Weapon Systems—A Scenario

Zura is the capital city of the Republic of Moria. It has the highest rate of violent crime in Moria, particularly in Doomlee, a county whose residents are largely people of color. Following government approval, the Zura Police Department (ZPD) started using AWS for policing and counterterrorism operations, notwithstanding critical reports from scientists indicating that these systems perform badly when it comes to identifying people with dark skin tones or shades.

So far, ZPD has only deployed AWS in Doomlee. In many cases, their use resulted in fatal shootings of suspects. ZPD has reported that since their deployment, no police officer has been killed in the line of duty in Doomlee and the crime rate has decreased considerably.

A local television network interviewed Doomlee residents regarding ZPD's use of AWS in Doomlee. Mr. Jones, the owner of a small grocery shop, said: "I think AWS are really effective. For the first time in a very long time, I haven't had a robbery in my shop."

Dontè, a teenager whose sixteen-year-old friend was killed by an AWS, said: "The killing of my friend was racially motivated. But when I say this, they look at me like I am crazy, they tell me race has nothing to do with it as machines see no color. AWS have increased deniability of racially motivated use of force by ZPD."

Mrs. James, a victim of domestic violence, said:

> When I called the ZPD emergency number telling them that my life was in danger, I expected police officers at my door. Sending AWS to police the situation made me feel a less valued citizen of Moria and less human. How come AWS are largely deployed in our poor communities, but in rich neighborhoods the ZPD sends human police officers? It appears the ZPD is saying that some communities deserve policing by human police officers while others are only fit for machines, iron and steel policing.

Local and international human rights organizations have described unlawful and violent acts committed by AWS in Doomlee as crimes against humanity as they consider such acts to be purposeful, widespread, and part of a systematic ZPD policy directed against residents of Doomlee.

While the case in Box 1 is fictitious, the scenario demonstrates a potential future that is anchored in the realities faced by people of color and those living in the Muslim world when lethal force is used by state agents. On the one hand, it reveals the concerns that have been noted on the potential of AWS to exacerbate racial bias and other forms of discrimination in society. On the other hand, some scholars take the view that AWS may improve the situation of the innocent whenever and wherever states use force.[41]

As emphasized above, contextualization is essential to fully understand the challenges posed by the use of AWS. The hypothetical case shows that, when evaluated in the context of law enforcement and counterterrorism operations, AWS deployment brings to the fore histories of racial bias and of impunity when lethal force is used unlawfully in the Muslim world and in communities of people of color, and reveals, more generally, a lack of moral responsibility over institutional racism associated with law enforcement. These three issues are addressed in turn in the following sections.

A History of Racial Bias in the Use of Lethal Force

The UN CERD Committee is the body of independent international experts who monitor the implementation of the CERD by its state parties.[42] In its 2020 report, particularly relating to the United States—one of the countries currently developing AWS—the CERD Committee noted various concerns regarding racial bias and the use of lethal force. It particularly noted "the continuing practice of racial profiling, the use of brutality and the excessive use of force by law enforcement officials against persons belonging to racial and ethnic minorities."[43] Similar concerns have been noted regarding other countries such as France, Israel, and the United Kingdom. In cases where people of color are involved, the CERD Committee has noted the disproportionate use of lethal force regardless of whether the target is armed.[44] It also expressed concerns that those who attempt to demonstrate peacefully against the racist use

of lethal force are often met with brutal and disproportionate use of force by state agents.

Crucially, the CERD Committee noted that the racist use of lethal force cannot be categorized as sporadic incidents committed by errant bad white police officers; rather, it is a matter of "systemic and structural discrimination [that] permeates State institutions and disproportionately promotes racial disparities against [people of color and ethnic minorities]."[45] The CERD Committee has thus noted that in all UN institutions—including the UNGGE that is currently discussing AWS—there should be condemnation of "modern day racial terror lynchings and calling for systematic reform and justice, and their statement on the protests against systemic racism."[46]

The CERD Committee has also expressed deep concerns over the lack of "appropriate accountability for and sanctions imposed [on] those responsible."[47] Thus even before the deployment of AWS, there exists an accountability gap when it comes to remedying violations of the rights of people of color and certain ethnic minorities. Yet with AWS on the horizon, things could get even worse in terms of obtaining racial justice.

The intense discussions and demand for racial justice that followed the murder of George Floyd were partly attributable to the fact that the public could see Minneapolis Police Officer Derek Chauvin committing the act. What if, as highlighted in the scenario above, Floyd had been killed by AWS? How would one even begin to characterize such an incident as constituting a racist use of lethal force when there is "no soul to damn" and "no body to kick?"[48] How easy will it become to dismiss racist use of force as machine error? Already, as will be discussed below regarding moral distancing from responsibility over institutional racism, sociologist Robin DiAngelo has expressed concern that "white fragility" not only leads many members of the white community to distance themselves from racist acts as a way of preserving their own moral character and standing, but also involves vigorous attempts to explain away violent racist acts by law enforcement officials—often by blaming the victim instead.[49] Likewise, political scientist John Emery has noted that reliance on emerging AI military technologies in the West's wars in the Middle East has created a distance between a morally wrongful act and its perpetrator.[50]

A History of Impunity in the Use of Lethal Force

In the United States and other countries where unlawful use of force by state agents against people of color has been prevalent, there have been complaints that such unlawful acts often go unpunished or entail no serious repercussions

for those responsible. Indeed, one of the grievances in the worldwide Black Lives Matter protests that followed the killing of George Floyd was that police officers had been and still were killing Black people with impunity.

On the global scale, history is replete with examples of Western governments and militaries committing war crimes in Africa, the Middle East, and elsewhere without accountability. Where offenders were prosecuted, there was no transparency, leaving victims unsatisfied. Calls for the prosecution of those who authorized the 2003 Iraq invasion have been ignored, even though the parties involved admitted that the justification proffered to the international community for such an invasion was proved to be false.

In another form of impunity for human rights violations, some Western governments have refused to fully account for slavery or compensate its victims, particularly people of color. In fact, many current governments have sought to maintain all the privileges that came with slavery. In 2021, the U.S. White House published a report that defended and sought to sanitize slavery.[51] The point is that refusal to account for violations, past and present, perpetrated against peoples from certain regions in itself perpetuates racial and religious oppression.

This history of impunity in accounting for violations of the human rights of people of color or those in the Muslim world is an important pretext that needs to be recognized and challenged when discussing the potential accountability gap created by the use of AWS, given their likely use in law enforcement and in counterterrorist operations in the Middle East.

Moral Distancing from Accountability and Responsibility

The impunity challenge relates not only to legal responsibility but also to moral responsibility for such violations. AWS will introduce yet another dynamic in the defenses that are often mounted when societies refuse to take moral responsibility for institutional racism associated with the use of force. In relational ethics, moral responsibility and accountability for violations or wrongdoing must be accepted. According to DiAngelo, the desire to distance oneself from moral blameworthiness, particularly from the negative effects of racism, is part of white fragility.[52]

White supremacy has undergirded colonialism, and it can be argued that the indiscriminate use of AWS in the Middle East, Africa, and other nations in the Global South is an extension of the historical legacy of discrimination against people of color and Muslims. From a sociological standpoint, refusal to take moral responsibility for both historical and current oppression of certain

peoples is part of the corpus of whiteness and white privilege. Yet white people, particularly those who see themselves as "progressives," who seek to distance themselves from moral responsibility over violations—or from not being part of the violators—are contributing to the continued oppression of people of color. White fragility explains away the targeting of people of color by attributing it to causes other than racism or racial prejudice. In other words, the moral stress to whiteness, particularly among "progressives," caused by indications that certain actions contribute to racial oppression, leads to a feeling of moral harm. Thus white fragility contributes to the current perception of racial oppression as something that can only be perpetrated intentionally and by bad white people. White fragility has led to a response to the George Floyd murder that this was a single case and not representative of a racialized society. Yet racism is not binary: even the good may be entangled in it.

The implications of DiAngelo's theory on this aspect of white fragility can also be applied to states' use of force against people of color, both domestically and abroad. In this context, the question arises: when AWS are used, what is the impact on the moral responsibility of the white general public in terms of the racist uses of force? The use of AWS may lead to a further distancing or erasure of moral responsibility. Racial oppression may no longer manifest itself visibly in the form of a white person. A machine killing a Black person will not only make it even easier to deny racism but will take the discussion about racism off the table. AWS, in this regard, may give racism a thicker cloak of invisibility. The argument may no longer be about "bad apples" in the police force but rather about machine error, making it difficult to address racism and the use of force by state agents.

The use of algorithms to kill displaces humans' moral responsibility for death by distancing them from the act of killing. In discussing the United States' use of two algorithms, bugsplat and SKYNET, in Iraq and Pakistan, Emery observes:

> The algorithmic logics of SKYNET and bugsplat both enable what they seek to constrain; namely making killing more palatable to the liberal conscience while deferring accountability for killing. . . . The systematic outsourcing of human judgement to algorithmic computation has the effect of absolving decision-makers of accountability for killing and justifying existing practices. These empirical probabilities towards death provide a cautionary tale for future military development in the field of AI. A techno-ethics that divorces us from the weight of taking lives in virtuous chaoplexic war is fraught with peril because it relinquishes due care to morally flawed coding. . . . What is at stake in these techno-practices of war is nothing less than the erosion of effective constraints on the

use of lethal force because the techno-rationalization of risk assessment has supplanted genuine ethical deliberation in contemporary conflicts.[53]

Further, as has been recognized by some sociologists, one powerful tool in racial and religious oppression is language construction. For example, DiAngelo explains that formulating discussions on racial oppression in terms of bad versus good people and intentional versus unintentional only serves to undermine discussions on racial oppression. Equally, in the case of emerging AI technologies like AWS, the construction and formulation of language have a sinister power in holding "that non-combatant deaths caused by Western militaries are only ever 'accidents' because we could never intentionally target civilians. The question of intention is brought to light by an overreliance on a technologic of algorithmic programming that not only rationalizes civilian deaths as a priori accidental but also raises the deeper question that these acts may be 'beyond intention.'"[54]

In documents on AWS submitted to the UNGGE, the U.S. government notes that in order to ensure that AWS help effectuate the intention of commanders,[55] it will take "practical steps to reduce the risk of unintended engagements."[56] It further posits that such an approach is consistent with the rules of international humanitarian law.[57] But its notion of reducing or minimizing unintended engagements is not found in IHL and human rights language. The United States defines "unintended engagements" as "the use of force resulting in damage to persons or objects that human operators did not intend to be the targets of [U.S.] military operations."[58] The United States further notes that such "unintended engagements" include "unacceptable levels of collateral damage beyond those consistent with the law of war, [rules of engagement], and commander's intent."[59]

Furthermore, the United States has submitted to the UNGGE that unintended engagements include accidental attacks on civilians[60] and attacks against targets whose factual context as it relates to participation in hostilities has significantly changed between the time of authorization and the point of engagement.[61] It has also referred to circumstances where there may be failures in AWS, meaning that resulting harm would not be part of the intention of persons deploying AWS. It has since defined a failure in a weapon system as "an actual or perceived degradation or loss of intended functionality or inability of the system to perform as intended or designed." Such "failures can result from a number of causes, including, but not limited to, human error, human-machine interaction failures, malfunctions, communications degradation, software coding errors, enemy cyber-attacks or infiltration into the industrial supply chain,

jamming, spoofing, decoys, other enemy countermeasures or actions, or unanticipated situations on the battlefield."[62]

Here too, these approaches by states must be examined with real victims in mind. For example, when a state talks of "unintended engagement," one ought to ask the question: unintended engagement with whom? Equally, when it talks about "accidental attacks on civilians" through AWS, one ought to ask: accidental attack on which civilian population? Contextualizing the situation and noting the identity of the likely victims can help explain why certain issues may be taken lightly or seriously. As has been noted by Peter Lee, "The greatest bias that a person might have—if they are even aware of the human propensity for bias—is the sense that it does not affect them."[63] As such, some may take lightly discussions about "unintended engagement" and "accidental attacks on civilians" by AWS because such engagements and accidents do not affect them or those close to them.

U.S. language construction on AWS goes to the root of fundamental and customary IHL rules on distinction and proportionality. The IHL rule of distinction prohibits indiscriminate attacks and is the basis of protection of the right to life in armed conflict. The obligation of belligerents is to refrain from indiscriminate attacks, not merely to reduce or minimize them. Likewise, regarding the IHL rule on proportionality, the obligation on belligerents is to refrain from conducting attacks that have disproportionate collateral damage, not merely to reduce or minimize disproportionality. In the use of new technologies such as AWS—weapons that are likely to be used in certain regions and against certain peoples—care must therefore be taken not to adopt or acquiesce in the construction of language that is irreconcilable with IHL provisions and fundamental human rights norms relevant to the use of force.

It is even more crucial to note, with regard to racial and religious oppression, that the United States is placing emphasis on AWS making mistakes and therefore not carrying out the intentions of those deploying them. There is thus already an attempt to distance those deploying AWS from responsibility or accountability for the harm that AWS may cause. Scientists have already warned that AWS will make mistakes, particularly in unstructured environments. Some of the algorithms, such as the abovementioned bugsplat, have already been deployed and caused immense suffering among the civilian population in the Middle East. To seek to continue deploying similar, or worse, technologies is not only to abandon the ethics of due care but, given the targets as described above, amounts to racial oppression. Yet there are already policies detailing issues of "unintended engagements" in a way that diffuses both legal and moral responsibility over unethical uses of AWS.

These legacies and gaps in our understanding and oversight of the roots and effects of AWS on human rights and the differential effects based on race and religion call for a new set of international norms and protections. One possibility, elaborated below, is an international compact on principles against discrimination and oppression. The norms and protections embodied in the internationally sanctioned concept must be extended to the inherent gaps embodied in the application of AWS in international warfare. But this requires, first, a recognition of the discriminatory implications of modern technology in warfare.

Conclusions and Recommendations: New Principles for Engagement

The use of AI military technologies such as AWS is among the critical factors that will influence geopolitics in the years to come. If AWS are not grounded in the human rights framework, they can contribute to an oppressive geopolitical system that is unfavorable to peoples who have been historically oppressed and dominated. As noted above, such a situation is not conducive to stable geopolitics.[64] Human history has repeatedly shown that racial and ethnic oppression begets the worst forms of violence that disturbs global peace and security. States should therefore carefully address questions of racial oppression and injustice associated with the development and deployment of AWS. This not only important for the sake of global peace and security but also for the protection of fundamental human rights. Human rights are always better protected during peacetime; measures that guide society away from the path of violence and war are therefore critical. Furthermore, racial oppression cannot be reconciled with the fundamental right to nondiscrimination.

It is important to contextualize the uses of AWS and identify the potential victims and perpetrators. When AWS are used in the context of law enforcement and counterterrorism operations, people of color and civilians in the Muslim world will be disproportionately affected. In formulating policy on the issue, states should therefore be aware that the AWS accountability gap has far-reaching consequences for racial justice: these groups of people may be denied the right to a remedy when state agents use force unlawfully through AWS.

In order to effectively address the racial oppression associated with AWS, in the discussion on this technology, stakeholders should start by acknowledging that it is not necessarily neutral but is racialized. As such, discussions on the racial implications of AWS should always be part of the agenda. Just as the African Commission for Human and Peoples' Rights recommended that

states should adopt the emerging notion of maintaining human control over AWS as a human rights principle, states should adopt a set of principles against discrimination and oppression as part of the international community's governance tools on AI technologies such as AWS.

Those principles would draw on fundamental human rights principles relating to human rights and customary norms of nondiscrimination. Their main tenet would be that in the development, use, and governance of AI technologies and in maintaining accountability for human rights violations related to AI technologies, robotics, and emerging technologies, states must commit to actively seek to eliminate all forms of unlawful discrimination such as those based on race, gender, or religion. In formulating these principles, states should take account of intersectionality, and decolonial and critical race theories, among others, that critique society, culture, and geopolitics to reveal and challenge power structures affecting inventions such as AWS within a historical context of racism and the endemic refusal to recognize its legacy effects. Under this conception, it should be possible to declare a weapon illegal per se if its development, use, and implications for accountability after use are inconsistent with the right to nondiscrimination. The concept of such principles—aimed at addressing the racial oppression and other forms of unlawful discrimination associated with certain AI technologies—is critical for the human rights project across the globe. If liberal democracies and advocates for human rights fail to recognize and address the challenges described above, the already attenuated international consensus around the objectivity and universality of human rights in the world today will be weakened even further.

Finally, for many states and stakeholders who have been calling for a new legally binding instrument on AWS, it is important to realize that the UNCCW, whose mandate is limited to situations of armed conflict,[65] is not an appropriate forum where all concerns—particularly those relating to racial oppression—can be addressed. AWS are likely to be used, in the context of law enforcement and counterterrorism, in situations where it is often the rights of people of color and civilians in Muslim communities that are violated. Insisting that an institution that cannot fully address the historically loaded impact of racial injustice on specific populations is the appropriate forum to discuss technologies such as AWS runs against the interest of racial justice and contradicts the idea of the principles proposed above. There needs to be a new, international covenant to defend those very rights. Such a commitment among states—through the UN or other multinational bodies—embodying the principles of nondiscrimination and addressing the accountability gap between those who design and decide on AWS and the implications of their use in the

field is a key step in the extension of human rights in the modern era. It could help raise awareness within the global community of concerned states and civil society, and move forward a much-needed debate on the human rights and discriminatory implications of modern techniques of warfare and surveillance.

Notes

1. While there is no agreed definition of AWS, this is the definition that is generally used. See, for example, A/HRC/23/47, Report of the United Nations Special Rapporteur on extrajudicial, summary, or arbitrary executions on lethal autonomous weapon systems (2013), www.ohchr.org/Documents/HRBodies/HrCouncil/Regularsession/session23/A-HRC-23-47_en.pdf.

2. See International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," May 12, 2021, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

3. Thompson Chengeta, "Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law," *Denver Journal of International Law & Policy* 45, 1, April 2020, https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1011&context=djilp; Human Rights Watch, "Mind the Gap: Lack of Accountability for Killer Robots," April 19, 2015, www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots.

4. Chengeta, "Accountability Gap"; Human Rights Watch, "Mind the Gap."

5. See the International Convention on the Elimination of All Forms of Racial Discrimination, adopted and opened for signature and ratification by General Assembly Resolution 2106 (XX) of December 21, 1965; entry into force January 4, 1969, in accordance with Article 19 (CERD).

6. Article 26 of International Covenant on Civil and Political Rights, adopted and opened for signature, ratification, and accession by General Assembly Resolution 2200A (XXI) of December 16, 1966; entry into force March 23, 1976, in accordance with Article 49 (ICCPR).

7. See Article 14 of the European Convention on Human Rights; Article 24 of the Inter-American Convention of Human Rights; Article 2 of the African Charter on Human and Peoples' Rights; Article 2 of the Arab Charter on Human Rights.

8. Article 6 of CERD.

9. Preamble of CERD.

10. Denise Garcia, "Stop the Emerging AI Cold War," *Nature* 593 (7858), p. 169.

11. Ibid.

12. See A/75/18, Report of the Committee on the Elimination of Racial Discrimination, Ninety-ninth session (August 5–29, 2019), 100th session, (November 25–December 13, 2019), para. 22.

13. Chengeta, "Accountability Gap;" Human Rights Watch," Mind the Gap."

14. A/HRC/23/47, 2013.

15. See S/2021/219, Letter dated March 8, 2021, from the Panel of Experts on Libya established pursuant to Resolution 1973 (2011), addressed to the President of the Security Council, para. 63, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement.

16. A/HRC/23/47, 2013.

17. See United Nations, "Machines Capable of Taking Lives without Human Involvement Are Unacceptable, Secretary-General Tells Experts on Autonomous Weapons Systems," March 25, 2019, www.un.org/press/en/2019/sgsm19512.doc.htm.

18. Australia, Israel, Russia, and the United States, among others.

19. Ron Arkin, "Lethal Autonomous Weapon Systems and the Plight of the Non-Combatant," *AISB Quarterly* 137 (2013), pp. 1–8.

20. See UNGGE, Background on LAWS in the CCW, n.d., www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.

21. ICRC, "ICRC Position on Autonomous Weapon Systems."

22. See CCW/MSP/2014/3, Report of the 2014 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), June 11, 2014; CCW/MSP/2015/3, Report of the 2014 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), June 2, 2015; Advanced Version of Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Submitted by the Chairperson of the Informal Meeting of Experts; CCW/GGE.1/2017/CRP.1, Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), November 20, 2017; CCW/GGE.1/2018/3, Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, October 23, 2018; CCW/GGE.1/2019/3, Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, September 25, 2019.

23. Robin DiAngelo, *White Fragility: Why It Is So Difficult for White People to Talk about Racism* (New York: Penguin, 2018), p. 14.

24. See the 2019 Report of the United Nations Working Group of Experts on People of African Descent, "Data for Racial Justice," https://undocs.org/en/A/HRC/42/59.

25. See #Saytheirnames, https://sayevery.name/.

26. Ibid.

27. Charles W. Mills, *The Racial Contract* (Cornell University Press, 1997), p. 122.

28. DiAngelo, *White Fragility*, p. 29.

29. Mills, *The Racial Contract*, p. 122.

30. Ibid., p. 40.

31. Shakir Mohamed, Marie-Therese Png, and William Isaac, "Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence," *Philosophy and Technology* 33, 4 (2020), p. 659.

32. Yarden Katz, *Artificial Whiteness: Politics and Ideology in Artificial Intelligence* (Columbia University Press, 2020), pp. 3–13.

33. See Abeba Birhane, "Algorithmic Colonisation of Africa," *Scripted* 17, 2 (2020); Mohamed et al., "Decolonial AI," p. 659.

34. Katz, *Artificial Whiteness*, pp. 6–7, 8–9.

35. Stephen Cave and Kanta Dihal, "The Whiteness of AI," *Philosophy and Technology* 33, 4 (2020), p. 687; See also Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (NYU Press, 2018); Jessie Daniels, "Race and Racism in Internet Studies: A Review and Critique," *New Media & Society* 15, 5, pp. 695–719; Jesse Daniels, "'My Brain Database Doesn't See Skin Color:' Color-Blind Racism in the Technology Industry and in Theorizing the Web," *American Behavioural Scientist* 56, 11, pp. 1377–93.

36. UN Special Rapporteur on contemporary forms of racism, Report, A/HRC/44/57, (2020), para. 48.

37. See Steve Garner, *Whiteness: An Introduction* (London: Routledge, 2007) p. 5.

38. See 2019 UNGGE Report, CCW/GGE.1/2019/CRP.1/Rev 2, p. 13.

39. Article 1(2) of the UN Convention on Conventional Weapons.

40. A/HRC/23/47, 2013.

41. See Arkin, "Lethal Autonomous Weapon Systems."

42. See the Committee on the Elimination of Racial Discrimination, www.ohchr.org/en/hrbodies/cerd/pages/cerdindex.aspx.

43. See A/75/18, CERD Report, 2019, para. 22.

44. Ibid.

45. Ibid.

46. See also CERD General Recommendations No. 31 of 2005 on the prevention of racial discrimination in the administration and functioning of the criminal justice system, No. 34 (2011) on racial discrimination against people of African descent, and No. 35 on combating racist hate speech (2013).

47. CERD General Recommendation No. 31.

48. See Peter Asaro, "A Body to Kick but Still No Soul to Damn: Legal Perspectives on Robotics," in *Robot Ethics: The Ethical and Social Implications of Robotics*, edited by Patrick Lin, George Been, and Keith Abney (MIT Press, 2010).

49. DiAngelo, *White Fragility,* pp. 9–38.

50. See John R. Emery, "Probabilities towards Death: Bugsplat, Algorithmic Assassinations, and Ethical Due Care," *Critical Military Studies* (October 2020), pp. 2–19.

51. Michael Crowley, "Trump's '1776 Report' Defends America's Founding on the Basis of Slavery and Blasts Progressivism," *New York Times*, January 18, 2021, www.nytimes.com/2021/01/18/us/trump-1776-commission-report.html.

52. DiAngelo, *White Fragility.*

53. Emery, "Probabilities towards Death," p. 16.

54. Ibid., p. 6. See also Patricia Owens, "Accidents Don't Just Happen: The Liberal Politics of High-Technology 'Humanitarian' War," *Millennium: Journal of International Studies* 32, 3 (December 1, 2003), pp. 595–616; M. Zehfuss, "Targeting: Precision and the Production of Ethics," *European Journal of International Relations* 17, 3 (October 1, 2010), pp. 543–66; J. Marshall Beier, "Short Circuit: Retracing the

Political for the Age of 'Autonomous' Weapons," *Critical Military Studies* 6, 1 (2008), pp. 1–18.

55. CCW/GGE.2/2018/WP.4, para. 1.

56. Ibid. Emphasis added in this and subsequent quotations.

57. CCW/GGE.2/2018/WP.4, para. 2.

58. United States Department of Defense Directive 3000.09, Glossary, p. 15.

59. Ibid.

60. CCW/GGE.2/2018/WP.4, para. 6.

61. Ibid.

62. Ibid.

63. Peter Lee, "Armed Drone Systems: The Ethical Challenge of Replacing Human Control with Increasingly Autonomous Elements," in *Ethics of Drone Strikes: Restraining Remote-Control Killing,* edited by Christian Enemark (Edinburgh University Press, 2020), p. 159.

64. Preamble of CERD.

65. See Article 1 (2) of the United Nations Convention on Conventional Weapons (UNCCW).