Autonomous weapons and digital dehumanisation

DIGITAL DEHUMANISATION is the process whereby humans are reduced to data, which is then used to make decisions and/or take actions that negatively affect their lives. This process deprives people of dignity, demeans individuals’ humanity, and removes or replaces human involvement or responsibility through the use of automated decision-making in technology. Automated harm occurs when these decisions negatively impact us. The digitisation of information about people, and the use of automated decision-making technology based on such digitised information, is not always problematic. However, it carries with it an increased risk of being dehumanising and of causing automated harm.

There are a range of different harms, at different levels of severity, which may result across the various uses of automated decision-making technology. For example, using algorithms to decide what grades are awarded to students can lead to unfair and potentially biased outcomes. The use of such technologies for banking, based on personal data such as where you live, your income, and your level of debt, coupled with your race, your gender, or your age, may result in an automated system denying you a loan or a mortgage. When algorithms and automated decision-making technologies are used for the administration of social welfare, you could be wrongfully denied benefits or erroneously flagged for fraud. In the areas of policing and criminal justice, the use of automated decision-making based on facial recognition technology can lead to wrongful arrest and incarceration, as can the use of predictive policing and criminal sentencing technologies.

The potential automated harm arising from autonomous weapons includes injury or death. As such, the digital dehumanisation caused by autonomous weapons is at the severe end of the scale of harms caused by automated decision-making or autonomous technologies. In the same way that police forces and border control forces use facial recognition technology based on biometric data (such as the distance between the eyes and the shape of the face) to decide that you are a specific individual who should be arrested, autonomous weapons use data acquired from sensors (such as weight, heat signature, or movement patterns) and process this data in order to decide whether to use force against you. Autonomous weapons do not ‘see’ you as a human being. Instead, you are ‘sensed’ by the machine as a collection of data points, and the machine uses its algorithm to fit these data points against its target profile. If this information matches or fits the target profile, the weapons system will apply force. There is no human involved in making this life or death decision. The digital dehumanisation that results from reducing people to data points based on specific characteristics also raises serious questions about how target profiles are created and what pre-existing data these target profiles are based on. It also raises questions about how the user can understand what falls into a weapon’s target profile and why the weapons system decided to use force.

Another aspect of the digital dehumanisation that we see with autonomous weapons is the distancing of human judgement and control from decisions about who or what to use force against, and how and when to use it. This means that people are further removed from targeting decisions, and further removed from the consequences of using force. Autonomous weapons also make it harder to understand who is responsible for any uses of force that do not comply with the rules of international humanitarian law (the body of law that applies in conflict) or with international human rights law.
Understanding and applying these legal rules requires a sophisticated and nuanced understanding of the context in which the use of force takes place. Autonomous weapons do not have the capacity to exercise human judgement over the kinds of complex scenarios that play out during war, or in domestic policing or border control scenarios. They also don’t have the ability to exercise doubt or to question themselves, as humans do.

Autonomous weapons are an example of digital dehumanisation at its most extreme. Giving machines the power to make life or death decisions undermines human dignity and denies us of our rights. Instead of being seen as people, people are processed as objects.

**WHAT ARE AUTONOMOUS WEAPONS SYSTEMS?**

With advances in artificial intelligence, specifically in the area of machine learning, there is a trend towards increasing autonomy in various functions of weapons systems. This means that weapons systems can carry out more tasks on their own, without the need for human involvement. Some of the areas where increasing autonomy is of particular concern includes critical functions of weapons systems such as target selection (deciding who or what to target) and the application of force (deciding whether or when to use force; for example, deciding whether to shoot a bullet or when to fire a missile). Systems that use machine analysis of information acquired from sensors to automatically select and engage targets, such that a human operator does not determine specifically where, when or against what force is applied, are of particular concern. These are what we mean by ‘autonomous weapons systems.’ In these systems, once the system is activated, there is a period of time where the weapons system can apply force to a target without additional human approval. The specific object to be attacked, and the exact time and place of the attack, are determined by sensor processing, instead of by an immediate human command. This means that no person is involved in making the decision to use force, or in deciding who or what force will be used against. When an autonomous weapon is activated, we do not know ‘specifically who or what it will strike, nor precisely where and/or when that strike will occur.” This raises numerous challenging questions from both a legal and an ethical standpoint, particularly around human control over the use of force, about accountability and responsibility for violations of international humanitarian law and international human rights law, and about allowing machines to make the decision to take human life.

**EXAMPLES OF WEAPONS SYSTEMS WITH AUTONOMOUS FUNCTIONS**

In recent years, we have seen the increasing development and use of a number of weapons systems with various concerning autonomous capabilities. These systems come in many different shapes and sizes. Some are drones or loitering munitions; some are unmanned ground vehicles, such as tanks. There are also unmanned surface vehicles, which can look like boats, or other unmanned sea vehicles, such as submarines." Two examples of systems of concern which are already in use include the STM Kargu-2 and the Kalashnikov Group’s KUB-BLA. The Kargu-2 is a loitering munition with autonomous flight capabilities and an automatic target recognition system. In 2021, a UN Panel of Experts reported that the Kargu-2 had been used in Libya, and had been ‘programmed to attack targets without requiring data connectivity between the operator and the munition.” The KUB-BLA, which is also a loitering munition, has reportedly been used by Russia in Ukraine. The KUB-BLA loitering munition is said to have ‘artificial intelligence visual identification (AIVI) technology for real-time recognition and classification of targets.”
HOW DO AUTONOMOUS WEAPONS WORK?

The kind of information that an autonomous weapon uses to select and engage a target depends on the types of sensors it uses, and what information those sensors collect. An autonomous weapon could use just one type of sensor, or it could use a mix of sensors. Examples of sensors include heat signature sensors, image processing cameras, and pressure sensors. Autonomous weapons use the information that they get from sensors and fit this information against a generalised target profile. If the information that the weapons system gets from the sensors does not fit its target profile, then it does not use force; it doesn’t fire a bullet or a bomb. However, if the information that the weapons system gets from these sensors matches the pre-programmed target profile, the weapons system will then use force against a target. That target could be a person or a car, for example, depending on the target profile that the weapon uses. What this means is that an algorithm makes the decision for the machine to use force and to engage a target based on the data that it gets from sensors, instead of a human (such as a soldier) making this decision. As the International Committee of the Red Cross has pointed out, this means that 'it is the vehicle or the victim that triggers the strike, not the user.' It also means that 'those who configure and deploy an AWS will not necessarily know the exact targets, location, timing or circumstances of the resulting use of force.'
ENDNOTES

* This paper was written by Dr. Catherine Connolly.


