***Amoroso, Daniele*: Autonomous Weapons Systems and International Law.** A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains. Baden-Baden: Nomos, 2020. ISBN 978-3-8487-6856-1. 304 pp. € 76.-; eISBN 978-3-7489-0953-8. € 76.-

Recent technological advancements, especially in the field of Artificial Intelligence (AI) and robotics, have significantly increased the probability that autonomous weapons systems (AWS), that is to say, weapons that select and engage targets without human intervention, may be deployed in future military operations. The process of increasingly outsourcing core tasks and competences to machines raises many different ethical and legal questions.

Given the importance of this highly topical issue it does not come as a surprise that a number of authors have already dealt with AWS from a legal and/or ethical perspective. That said, Daniele Amoroso's recent piece clearly represents an outstanding contribution to the broader debate.

As the title of the book indicates, the author primarily intends to address legal issues. In doing so, however, he pays due regard to the fact that legal considerations, especially when it comes to international humanitarian law (IHL), do not stand alone but are intertwined with ethical concerns that have always informed and shaped humanitarian norms. By the same token, Amoroso also bears in mind relevant political developments as a contextual basis of his legal analysis. Thus, while his treatise is generally about international law, it neither ignores other (related) fields, such as ethics and international relations, nor the complexity of autonomous weapons systems as such.

Chapter 1 is composed of well-written introductory remarks on AWS by *inter alia* addressing questions relating to their definition, their history, and the term 'autonomy' in weapons systems in general. Even though there is no official definition of AWS in international law, the definition provided by the International Committee of the Red Cross (ICRC) is widely accepted among states and legal scholarship. The ICRC denotes autonomous weapons systems as 'any weapon system that once activated can select and attack targets without human intervention'.[1] This definition can fairly be described as an umbrella term that is able to cover a plethora of weapons systems, some of which have even been deployed in contemporary military operations, such as air defence systems and sentry weapons. The author also uses this definition but likewise addresses the definition of AWS provided by the United Kingdom Ministry of Defence (UK MoD), the United States Department of Defense (US DoD), and the Campaign to Stop Killer Robots, a coalition of

[1] ICRC, Views of the International Committee of the Red Cross on autonomous weapon system, paper submitted to the Meeting of Experts on Lethal Autonomous Weapons Systems, 11 April 2016, 1.

DOI 10.17104/0044-2348-2021-3-873

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

various non-governmental organisations strongly advocating a complete ban of AWS. While the UK MoD establishes quite strict criteria for AWS by denoting them as weapons that are 'capable of understanding higher level of intent and direction'[2] and hence being 'capable of understanding higher level of intent and direction',[3] all other stakeholders prefer a rather broad definition by focusing on the capacity to select and engage targets without further intervention by a human operator. Most importantly, the author clarifies that the rather broad definition advanced by the ICRC, the US DoD, and the Campaign to Stop Killer Robots, actually cover already existing weapons systems, such as air defence systems, active protection systems, robotic sentry weapons, guided munitions, and loitering weapons (pp. 18-21).

It would have been interesting to read more about current defence projects of key military leaders, such as the US, China, and Russia in order to adequately appraise the essence and nature of future military operations. However, account must be taken of the fact that most military projects are confidential and gaining reliable and meaningful information is difficult. Also, it would have been helpful to emphasise more clearly that autonomy in weapons systems does not necessarily refer to specific platforms of weapons, such as aerial vehicles or vessels. Autonomy in weapons systems will also yield interoperable systems-of-systems, which can be briefly described as a compound of complex, inter-operable weapon systems interacting with each other (a factor that is briefly addressed later in the book), significantly increasing the pace of military operations, which in turn will confront human operators with even more legal and ethical challenges. However, though it would have been interesting to read more about these aspects, the quality of the book is in no way negatively affected by it.

Chapter 2 sets out to explore the 'legality test' for autonomous weapons systems by addressing core provisions of international humanitarian law, such as the principles of distinction, proportionality, and precautions in attack. The author describes 'proportionality' as a distinct principle of humanitarian law. While there is much support for this line of argumentation in international law, some authors (such as *Heintschel von Heinegg*) contend that IHL does not embrace a general principle of proportionality but rather entails very specific rules explicitly referring to proportionality in attack. For the most part, however, this is a purely academic debate, which as such does not materially affect the author's highly insightful reflections on the content and application of the proportionality rule in the context of AWS and their potential use in practice. According to the author, proportionality assess-

2 UK MoD, Joint Doctrine Note 2/11, 30 March 2011, 14.
3 UK MoD, Joint Doctrine Note 2/11 (n. 2).

 DOI 10.17104/0044-2348-2021-3-873

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

ments undertaken by AWS are particularly problematic, especially in dynamic targeting scenarios where unforeseen circumstances may arise. This does not mean, however, that AWS are considered unlawful per se (in the context of the proportionality debate) but each military scenario has to be assessed individually (pp. 76-96).

In the same chapter, the author also considers human rights law in the context of AWS, especially with regard to the right to life. The latter is basically addressed in a two-fold perspective; first, in the context of friendly fire and, second, in the context of domestic riot control. This analysis is very helpful as it clearly contrasts the different questions arising from both humanitarian and human rights law. Without doubt, the exact relationship between humanitarian and human rights law has always been contentious and different positions have evolved throughout the years. The author deliberately omits a deeper examination of this issue, which would have expanded the monograph and would have distracted from the core legal questions anyway. But it is understood here that the author supports a complementary approach, according to which the two legal regimes are by no means mutually exclusive. It might have been interesting to read more about the core legal provisions relevant for the deployment of AWS in non-international armed conflicts as well but, again, such analysis would have expanded the purpose of this book.

At the end of the chapter the author concludes that – depending on the relevant system deployed and depending on the relevant operational environment – different types and degrees of human involvement may be legally required. What the author convincingly makes clear is that generalisable conclusions in the context of humanitarian and human rights law and the AWS debate may be difficult to draw. What the author offers instead is a quite unique 'legality test' that establishes particular categories (so-called prongs) of abstract scenarios where AWS come to use. He then goes on to ascertain whether – provided that all the parameters established in these abstract criteria are met – the deployment of AWS would be in line with the law. Though one might consider the analysis of rather abstract scenarios an over-simplification of a highly complex topic, it ultimately provides the reader with a very helpful (initial) orientation.

Chapter 3 addresses one of the most contentious topics related to the use of AWS: the accountability gap. First, the effects of AWS might be difficult to predict and to understand for humans, especially when Artificial Intelligence/Machine Learning comes into play. The 'black box phenomenon' of AI refers to the fact that a system, device, or computer program may reveal both the input and the output but the underlying process that has actually led to the relevant output remains unknown to the human brain. Humans may

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

not be entirely capable of understanding a particular system, let alone predict its effects. Second, especially in the realm of AWS, many people are involved in their design, development, procurement, and deployment. In case a weapons system causes some kind of damage either to humans or objects, the question arises of who can actually be held accountable for it.

The first legal regime the author pays closer attention to is International Criminal Law. He analyses modes of direct responsibility including questions relating to accessory modes of liability and discusses the participation to a particular crime by software developers as well as Joint Criminal Enterprise, a mode of responsibility that has hitherto been denied by the International Criminal Court (ICC) but embraced by the International Criminal Tribunal for the former Yugoslavia (ICTY) on various occasions. One of the most difficult aspects regarding the deployment of AWS, however, is the mandatory *mens rea* element, a question the author addresses carefully in the same section and on several other occasions in Chapter 3. The ICC-Statute requires that crimes be committed – unless otherwise provided – with intent and knowledge. It will be most difficult to prove that, for example, a software developer, or any other person involved in the process of designing, developing, or deploying AWS, has intentionally undertaken defective programming in order to commit (or contribute to) a crime within the jurisdiction of the International Criminal Court. Thus, it will be most difficult to prove that a person has either committed or contributed to the commission of an international crime in the context of deploying AWS.

Due to the difficulties of establishing the *mens rea*-requirement, Amoroso also addresses crimes committed with *dolus eventualis*. In the context of international criminal law, *dolus eventualis* means that a crime is committed without a concrete intent but that the perpetrator 'accepts' the consequences of the crime that may occur, such as the killing of civilians. As shown earlier by Amoroso, this seems to be a likely scenario in the context of the use of AWS. The ICC, however, after some 'jurisprudential swinging' (a hint is made here to the famous *Lubanga* Case[4]), has ruled out the possibility that crimes committed with mere *dolus eventualis* might be justiciable under the Rome Statute. The author concurs with this position and presents convincing arguments here; however, it would have been interesting to read more about the overall controversial debate as to whether *dolus eventualis* could be covered by the ICC's jurisdiction (pp. 131-146).

The author also addresses questions relating to state responsibility, corporate, product, and non-fault liability. While various authors contend that the

4 ICC, *Prosecutor v. Thomas Lubanga Dyilo*, Appeals Judgment of 1 December 2014, ICC-01/04-01/06 A 5, para. 449.

 DOI 10.17104/0044-2348-2021-3-873

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

law on state responsibility does not pose any problems in relation to the deployment of AWS because the Articles on State Responsibility (ASR) do not prescribe the fulfilment of a particular *mens rea* element, the author cautions that the Draft Articles are only 'secondary' norms on state responsibility, whereas a particular mental element could indeed be envisioned by the primary norm in question 'whose alleged violation is at stake' (p. 147).

Chapter 4 is not just beautifully written but also particularly thought-provoking. Here, Amoroso addresses ethical concerns regarding the deployment of AWS and places them in context of core legal questions. The deliberations include a carefully analysis of the principle of human dignity, a concept not only forming part of an ethical discussion but an arguably legal norm that shapes and restrains the interpretation of other norms of international law. Human dignity is not only contained in the Preamble of the Charter of the United Nations but it can also be found in various human rights treaties. The European Convention on Human Rights does contain an explicit rule on human dignity but reference to the concept has been made by the European Court of Human Rights in *Yaroslav Belousov v. Russia*, for example.[5] As already indicated, the concept of human dignity forms part and parcel of an ethical discussion (the author refers to Immanuel Kant's 'Objektformel'), which has also been reflected in a judgement rendered by the German *Bundesverfassungsgericht*[6] in 2006. The author convincingly demonstrates that, in order to be in compliance with the principle of human dignity, human agency over targeting decisions must be preserved even though the type and degree of human involvement still remains unclear and highly depends on individual circumstances (pp. 165-172). By the same token, Amoroso addresses the Martens Clause and its relevance for the discussion on AWS. The Martens Clause also refers to 'the principles of human dignity' but also encapsulates a reference to 'dictates of the public conscience'. The author clarifies that the Martens Clause is more than a simple manifestation of ethical considerations. On the contrary, the Martens Clause 'has gradually acquired pride of place within the international legal architecture' (p. 174). The International Court of Justice, for example, has described the Martens Clause 'an effective means of addressing the rapid evolution of military technology'[7] (p. 173).

5 See ECtHR, *Yaroslav Belousov v. Russia*, Judgment of 6 March 2017, Appl. Nos 2653/13 and 60980/14, para. 92.

6 *Bundesverfassungsgericht*, Judgment of the First Senate of 15 February 2006, BVR 357/05, para. 134.

7 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1966, ICJ Reports 1966, 226, para. 78.

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

Chapter 5 wraps up the discussion by providing information on the current endeavour of (at least some of) the States Parties to the Conventional Weapons Convention to finally find a path towards a future regulation of AWS. In light of his analysis, the author concludes that preserving human control in the deployment of AWS is both legally and morally required. The author also concedes, however, that the type and degree of control may differ depending on the relevant weapons system deployed, the relevant target in question, as well as the operational environment. To learn about the different positions taken by States Parties on the question of human control (some States Parties even contest the term human control altogether and favour a different wording instead, such as 'human judgement') is both interesting and illuminating. At the end of Chapter 5, Amoroso sketches out how a future regulation could be designed by establishing various (rather abstract) 'scenarios' which would require different types and levels of human control. Irrespective of whether these ideas will ultimately be taken up in practice, they are immensely helpful for lawyers, policy makers, interested civil society groups, and all those dealing with AWS to better come to grips with one of the most challenging topics of our times (pp. 217-260).

This present monograph represents an outstanding contribution to a delicate field. It should be read by everyone who is interested in the AWS debate. Probably, the central message to be drawn from it is that, when it comes to autonomous weapons systems, a 'one-size-fits-it-all' solution will be impossible to achieve. The added value of Amoroso's book is that it provides the reader with a viable orientation regarding both the defining elements and the manifold intricacies of the current AWS debate.

Elisabeth Hoffberger-Pippan, Berlin

 DOI 10.17104/0044-2348-2021-3-873

https://doi.org/10.17104/0044-2348-2021-3-873 https://www.inlibra.com/de/page/agb - Open Access - CC BY-SA