

The ‘Technology War’ and International Law: A Legal Perspective on New Technologies Used in the Ukraine Conflict

Steven van de Put & Marten Zwanenburg

Abstract

This chapter will examine how the law deals with new technologies employed on the battlefield, using examples from the conflict in Ukraine. It is submitted that from a legal perspective, new technologies can fit into one of three distinct categories. The first category consists of technologies that represent a gradual advancement and therefore fit the existing legal obligations. The second concerns technologies that international law is able to accommodate through the use of interpretative methods. Lastly, some technologies might require the adoption of new legal obligations. Rather than focus specifically on one particular technology, this chapter will examine how international law can ‘catch up’ with technological developments on the battlefield. In this way, it offers insight into how international law can incorporate new technological developments, providing relevant considerations for future conflicts. As armed conflict seems to, unfortunately, always be a great driver for innovations, it will remain relevant for states to consider how these technologies should be approached from a legal perspective.

Keywords: New technologies, International law, Armed conflict

1. Introduction

One of the striking features of the fighting that has been taking place in Ukraine since February 2022 has been the large-scale employment of technology on the battlefield. New or at least recent technology has been used by both sides, in some cases to great effect. Examples include the use of hypersonic missiles, the large-scale use of satellite technology, cyber operations and Artificial Intelligence (AI). Ukraine’s Minister of Digital Transformation has gone so far as calling the conflict a ‘technology war.’¹

The fact that new and emerging technologies and methods for employing them are tested in an armed conflict is not new. States have always been keen to trial new

¹ Arhirova, “Minister: Ukraine will beat Russia in war of technologies.”

means and methods of warfare in an actual combat environment. Earlier examples are the Vietnam War and the conflict in Syria.² It has been suggested however that the scale on which technology is used in the conflict in Ukraine is unique.³

The use of new and emerging technology during an armed conflict raises many questions. Some of these are legal in nature. Such technology may raise questions concerning the application and interpretation of existing law in relation to such technology. It may not be clear how to ‘translate’ existing rules to a certain technology (means) or how that technology is used (method). Questions may also arise concerning whether new rules are needed to prohibit or regulate new technology. Such questions may come into sharper focus when the use and effects of a particular technology are witnessed in an actual conflict.⁴

Lack of clarity concerning the application of the law to particular technologies is problematic for states for several reasons. First, it makes it more difficult for them to ensure that they respect the obligations under international law which they have entered into. If it is unclear what these require of the state, that state may unintentionally breach those obligations and thereby incur international responsibility. Lack of clarity concerning the applicable law also leads to instability in the sense that states are less clear about what they may expect from others, including their opponents and their allies. This increases the risk of misunderstandings and misinterpretations, and complicates holding states and other actors accountable.

This chapter examines how states can deal with legal questions arising from the use of new and emerging technology, drawing on the conflict in Ukraine. It will be argued that three main categories of technology can be identified in this context. First, there are technologies that can be regulated by existing law without problems. Second, there are technologies that raise questions concerning the applicable law, but those questions can be answered satisfactorily by interpreting the law. Third and finally, a particular technology may require the adoption of new rules. It will be argued that these three categories provide a useful analytical framework when considering how to deal with the legal regulation of new technologies used in armed conflict. However, they are not watertight compartments. In some cases there may be reasonable arguments for placing a technology in more than one category, and in any event over time the majority view in the international community

² Beecher, “All sides test their arms in Vietnam.”; Sharkov, “Russia is using Syria to test its next generation of weapons.”

³ See Arhirova, “Minister: Ukraine will beat Russia in war of technologies.”

⁴ Crootof identifies four ways in which new technology can be legally disruptive. In addition to the two mentioned here and which are the focus of this chapter, these are a) technology that significantly changes the way that law is created or used and b) technology that highlights existing ambiguities in existing law. Crootof, “Regulating new weapons technology.”

concerning a particular technology may change concerning in which category such technology belongs.

The main purpose of the chapter is to provide an analytical framework for considering the interaction between the use of new technologies in armed conflict and international law. The chapter does not aim to provide an in-depth analysis of the regulation under international law of specific technologies used in armed conflict. It also is not geared toward providing recommendations on how states should deal with particular technologies from a legal perspective, although the analytical framework provided may help states in formulating their views on this. The chapter also does not aim to provide an exhaustive overview of the use of new technology in the conflict in Ukraine. The conflict is rather used to illustrate the broader issues described above.

2. Applying existing law – applying old law to new technology

Questions concerning how the law should deal with technology are not new. This includes the situation in which such technology is used in the military domain. Many publications on this topic begin by referring to attempts to outlaw the use of the crossbow in the Medieval Age.⁵ It has been pointed out however that nowadays, technological change takes place much faster and that more technologies have a great impact, acting as a 'game changer'.⁶

When a new means or method of warfare is developed, the first question to be asked from a legal perspective is whether it challenges the existing legal framework. This section of the article will discuss how existing law can deal with new technology, drawing on examples from the Ukraine conflict. After briefly describing the starting point for applying international law to new technology, it will identify three categories of technologies. First, there are technologies that can be regulated by existing law without problems. Second, there are technologies that raise questions concerning the applicable law, but those questions can be answered satisfactorily by interpreting the law. Third and finally, a particular technology may require the adoption of new rules.

⁵ See E.G. Shereshevsky, "International humanitarian law-making and new military technologies."

⁶ McLaughlin and Nasu, "Introduction: Conundrum of new technologies in the law of armed conflict."

2.1 Existing legal obligations

Within international law, the starting point that existing law applies to new means and methods of warfare is broadly accepted. Most famously, the International Court of Justice (ICJ) took this approach in the *Threat or Use of Nuclear Weapons Advisory Opinion*. In the arguments that some states made before the court, they advanced the viewpoint that the court would be engaging in law-making if it considered the legality of nuclear weapons. The court rejected this view, by stating that ‘the contention that the giving of an answer to the question posed would require the Court to legislate is based on a supposition that the present corpus juris is devoid of relevant rules in this matter.’⁷

The court also held that the existing rules of International Humanitarian Law (IHL) apply to ‘all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.’⁸

2.2 Applying existing law without the need for further interpretation

As was set out above, the starting point when new technologies are introduced on the battlefield is that existing legal obligations regulate those technologies. The question then arises whether those obligations can be applied without difficulty.

It is not the case that all new technologies provide an ill fit with the existing legal framework. Some developments might, for all intents and purposes, actually match with the existing legal framework. Whereas the conflict in Ukraine has, in many cases, provided some legal challenges, this is not the case for all of the technological developments we have seen used in this conflict.

When applying this approach to specific technologies employed in Ukraine, several examples can be given. Firstly, we have seen the use of hypersonic missiles. It has been reported that Russia has employed its Kinzhal missile, a modified version of the Iskander short-range ballistic missile that is launched from an airplane.⁹ These are missiles that are able to travel at more than five times the speed of sound, providing operational benefits for the state employing them.¹⁰ Their speed leads to them being difficult to detect on radar systems and makes it near impossible to effectively intercept these weapons.¹¹

⁷ Legality of the threat or use of nuclear weapons, par 18

⁸ *idem*, par 86.

⁹ Ismay, Mpoke Bigg, and Kramer, “Questions surround Russia’s use of hypersonic missiles in its latest attack.”

¹⁰ Brockman and Schiller, “A matter of speed? Understanding hypersonic missile systems.”

¹¹ Al Jazeera, “What are the hypersonic missiles Russia is using in Ukraine?”

When considering these weapons from a legal perspective, it however becomes clear that they do not pose any fundamental challenge to the application of the existing legal framework. Whereas some adaption or gradual changes might be necessary, they do not require a fundamental new obligation or new interpretation. An example here can be seen in the considerations under the *ius ad bellum*, where the use of hypersonic weapons may have a significant impact on how the law is applied. Under the *ius ad bellum*, the right of self-defence is one of the exceptions to the prohibition on the use of inter-state force. One of the requirements for a state to be able to invoke that right is that there is an armed attack. There is broad, albeit not general, support for the view that an 'imminent' armed attack also triggers the right to self-defence. As Gill states, the speed of hypersonic weapons 'would conceivably push the moment in which it would be perceived to be necessary to conduct a pre-emptive strike forward – well beyond what is currently thought of interceptive or anticipatory self-defence – into the realm of a preventive strike.'¹²

This is because the speed of the weapon could impact gauging when a defensive response is necessary.¹³ This will affect the application of the law but not necessarily the law itself or even its interpretation. Under the *ius in bello* or IHL, it has been generally accepted that the principles of targeting would still govern the use of these weapons. As these weapons do not introduce any fundamental new characteristics, the existing legal framework would still apply and govern their use.¹⁴

A second example concerns the use of naval drones by Ukraine. In April 2023, Ukraine used unmanned maritime systems, also referred to as 'naval drones,' to attack the Russian Black Sea Fleet in the Crimean port of Sevastopol. Russia claimed it repelled the attack.¹⁵ Navies have a long tradition of using so-called fire ships to attack enemy fleets. A famous historical example of this would be the British use of such ships in sinking the Spanish Armada in 1588.¹⁶ Naval drones can be seen as a successor of these fire ships. As a general rule, states have simply recognised these as weapons and have not yet gone as far as recognising this as a specific category of vessels. This entails that these do not necessarily need navigational rights.¹⁷ Instead, as states interpret these as a form of weapon within the existing regime, they would still be governed by the existing rules regarding naval targeting, and these have so far been interpreted according to the prevalent legal obligations.¹⁸

¹² Gill, "The *Ius ad Bellum* Anno 2040: An essay on possible trends and challenges."

¹³ Gill, "The *Ius ad Bellum* Anno 2040," 35.

¹⁴ Dinstein, "Air and missile warfare under International Humanitarian Law."

¹⁵ Reuters, "Russia says it repels naval drone attack on Sevastopol."

¹⁶ Royal Museums Greenwich, "Launch of fireships against the Spanish Armada, 7 August 1588."

¹⁷ Tuckett, "What's in a name? Getting it right for the naval "drone" attack on Sevastopol."

¹⁸ International Institute of Humanitarian Law. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, par 38-45.

A third example concerns the use of biometrics. Although there are no provisions in IHL expressly regulating this technology, IHL applies to its use during armed conflict.¹⁹ A broad range of uses of this technology, both in peacetime and during armed conflict, most notably concerning the gathering and storing of biometric data of civilians, would also be governed by human rights law. In this case, it is especially relevant to consider the practice of Russia in so-called ‘filtration camps.’ These are camps set up by Russia where ‘filtration’ of Ukrainian citizens in regions under Russian occupation takes place, often before transferring those persons to Russia. Filtration is a form of compulsory security screening, typically involving the collection of biometric data of the civilians concerned.²⁰

So far, it has been reported that Russia has gathered a substantial amount of biometric data on civilians within the territories which it has occupied.²¹ An argument could be made that this would be a violation of IHL, for example, because this does not respect their persons or because it constitutes obtaining information through coercion.²² It might be more relevant however to consider the more comprehensive legal obligations under human rights law in this context. Within the context of these filtration camps, it could be established that Russia has human rights obligations vis-à-vis the persons in those camps, leading to the relevance of such considerations.²³ This article will not address the issue of the interaction between IHL and human rights, other than noting that the starting point of such interaction is that the two fields of law complement each other.²⁴

Analysing the use of such technologies from a human rights perspective offers some insight into how international law governs their use. Both Ukraine and Russia were parties to the European Convention on Human Rights (ECHR), although Russia ceased to be bound on 16th September 2022 following Russia’s exclusion from the Council of Europe. Both states continue to be parties to the International Covenant

¹⁹ Graf, “Between accuracy and dignity: Legal implications of facial recognition for dead combatants.”

²⁰ Human Rights Watch, “We had no choice: ‘Filtration’ and the crime of forcibly transferring Ukrainian civilians to Russia.” For a legal analysis of the camps, see Kalandarishvili-Mueller, “Civilians are protected under GC IV 1949: The illegality of Russian filtration camps under IHL.”

²¹ Kalandarishvili-Mueller, “Civilians are protected under GC IV 1949: The illegality of Russian filtration camps under IHL.”

²² Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, art 27, 31.

²³ It has been accepted that human rights jurisdiction can also be outside of a state’s territory. This would be conditional on established effective control over an area or through state agent control, and within the context of the filtration camp Russia arguably has both.

²⁴ For further analysis see inter alia e.g. Gill, “Some thoughts on the relationship between International Humanitarian Law and International Human Rights Law: A plea for mutual respect and a common-sense approach.”; Droege, “The interplay between International Humanitarian Law and International Human Rights Law in situations of armed conflict.”

on Civil and Political Rights (ICCPR).²⁵ Most relevant here would be Article 8 of the ECHR and Article 17 of the ICCPR, guaranteeing the right to privacy. Under these articles, any gathering of biometric data would have to be both proportional and have a lawful basis, preventing the arbitrary deployment of such technologies.²⁶ Human Rights Watch has concluded that the Russian data collection practices in the context of the filtration process raise serious concerns around respect to privacy, as well as data protection.²⁷

In this way, some technologies might simply represent operational advancements or new uses of concepts, means and methods, to which existing international law can be applied without particular problems. Yet, this is not the case for all new (uses of) technology within the current conflict. In some cases, it might be necessary for states to further define existing obligations to ensure that they remain relevant. The following paragraph will offer some considerations in this context.

2.3 Interpreting existing legal obligations

A second category concerns new (uses of) technologies that introduce fundamental new characteristics, yet these characteristics are still able to be accommodated by the existing legal obligations. In these situations, it is often not the case that the use of these new technologies can be accommodated in a straightforward manner. Applying existing law may not be a good fit with the new technology, or with a particular use of that technology. That does not necessarily mean that the existing law cannot be applied, however. Rather, states may come to new interpretations of the law in order to 'translate' legal obligations to adequately regulate new technologies.

This is nothing new. Indeed, interpretation of the law is central to the application of international law. International law itself provides tools for such an exercise, notably in the form of broadly accepted rules of treaty interpretation which have been laid down in the Vienna Convention on the Law of Treaties. The central rule is that a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.²⁸ One of the things to be taken into account is the subsequent practice in the application of the treaty by the parties.²⁹ Particular

²⁵ See, for some of the effects of Russia leaving; Emtseva "The withdrawal mystery solved: How the European Court of Human Rights decided to move forward with the cases against Russia."

²⁶ Zwanenburg and van de Put "The use of biometrics in military operations abroad and the right to private life."

²⁷ Human Rights Watch, "We had no choice: 'Filtration' and the crime of forcibly transferring Ukrainian civilians to Russia."

²⁸ Vienna Convention on the Law of Treaties, Article 31 (1).

²⁹ Vienna Convention on the Law of Treaties, Article 31 (3) (b).

treaties or even subdisciplines of law also include rules that are particular to that treaty or subdiscipline that may play an important role in interpretation. For example, several IHL treaties include a version of the so-called ‘Martens clause.’ This clause is included, with minor variations in wording, in several IHL treaties. This includes Article 1 of the first Additional Protocol to the Geneva Conventions, which reads: ‘In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.’³⁰

The ICJ has considered that this clause ‘has proved to be an effective means of addressing the rapid evolution of military technology.’³¹ Although the precise meaning and role of the Martens clause is the subject of controversy, one way in which it has been understood is in informing the interpretation of rules the application of which is unclear.³² As stated in the judgment of the ICTY Trial Chamber in the Kupreskić case: ‘this Clause enjoins, as a minimum, reference to those principles and dictates any time a rule of international humanitarian law is not sufficiently rigorous or precise: in those instances the scope and purport of the rule must be defined with reference to those principles and dictates.’³³

At the same time, ‘translating’ existing law to make it compatible with a new (use of) technology has its challenges. For example, a particular interpretation may raise problems when that interpretation is used in another context. There may be cases where the interpretation of the law is so far-reaching that the law is stretched to breaking point. And different states may not agree on a particular interpretation of the law, so that there is not one ‘authoritative’ interpretation. These are some of the reasons why such an exercise has been referred to as more art than science and requires caution.³⁴

The conflict in Ukraine offers a number of examples of the above. One of them is the use of cyber operations. The use of such operations, or at least what is referred to as ‘hard’ cyber operations, appears to have been more limited in Ukraine than many experts had expected. This does not mean that cyber operations have not

³⁰ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 1 (2).

³¹ Legality of the Threat or Use of Nuclear Weapons, par 78.

³² See for an analysis of the Martens Clause inter alia Meron, “The Martens Clause, principles of humanity and the dictates of public conscience.”; Cassese, “The Martens Clause: Half a loaf or simply pie in the sky?”

³³ Prosecutor v. Kupreskić, par 525.

³⁴ Corn, “Cyber operations and the imperfect art of “translating” the law of war to new technologies.”

played an important role in the conflict, however.³⁵ Such operations raise a variety of questions under IHL.

One of these concerns is how to conceptualise data, a vital element of cyber operations, for the purposes of IHL. When considering legal targets, IHL makes reference to the notion of military objectives. Military objectives are defined in Article 52(2) of the first Additional Protocol to the Geneva Conventions (AP I): 'In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.' This definition is binding on Ukraine and Russia since they are both parties to AP I, but it is also considered as reflecting customary international law, thus also binding states not parties to AP I.

Under the abovementioned definition, something can only be a legitimate military objective if it is first an 'object.' It is unclear however if digital data qualifies as such an object.³⁶ Traditionally, only tangible objects have been considered to be 'objects' in the sense of IHL. States could clarify whether they consider the term should also extend to immaterial objects such as digital data. Unfortunately, states appear to hold different views on this. Certain states, such as Denmark and Israel, have clarified that they do not see data as an object in the sense of IHL.³⁷ In contrast, other states including Germany and Norway, hold the view that at least some types of data should be considered as objects under IHL.³⁸ Consequently, no shared interpretation has yet been reached of the term 'object' that provides clarity on the status of data under IHL.³⁹

Such clarity is necessary in evaluating whether certain cyber operations in the Ukraine conflict respect the principle of distinction. This principle provides that civilian objects may not be attacked.

In January 2023, a data wiper malware called CaddyWiper was used against a Ukrainian news agency, Ukrinform, deleting information on that organisations' systems. This cyber operation was attributed to what is allegedly a unit of the

³⁵ See e.g. Ducheine, Pijpers, and Arnold, "The 'next' war should have been fought in cyberspace, right? An analysis of cyber-activities in the 2022 Russo-Ukraine War."

³⁶ Pomson, "Objects? The legal status of computer data under International Humanitarian Law."

³⁷ Ministry of Defence of Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 292; Schondorf, "Israel's perspective on key legal and practical issues concerning the application of International Law to cyber operations," 401.

³⁸ Federal Government of Germany, *On the Application of International Law to Cyberspace*, 7; Norway, *Manual i Krigens Folkerett*, par 9.58.

³⁹ NATO CCDCOE, "Qualification of Data as an Object under IHL."

Russian military intelligence organisation GRU.⁴⁰ If the Ukrinform data is considered as an object, then it could be argued that this constituted a violation of the principle of distinction.

This example also illustrates another controversy concerning the application of IHL to cyber operations. This is the question of whether cyber operations can constitute an ‘attack’ in the sense of IHL. A number of IHL rules, including the prohibition of attacking civilian objects, apply only to ‘attacks.’ The term ‘attacks’ is defined in Article 49 AP I as ‘acts of violence against the adversary, whether in offence or in defence.’ There is no international agreement on the question of whether cyber operations, in particular cyber operations that do not cause physical damage, constitute an ‘attack’ in this sense.⁴¹ If they do not, then the use of Caddywiper malware to delete data would not be governed by IHL rules concerning ‘attacks’ and, as a consequence, could not violate these rules.

The ambiguity concerning whether data constitutes an object and when cyber operations constitute an ‘attack’ can be addressed by states interpreting existing law. This is why these questions are discussed here to illustrate the second category of the three described in this chapter. This is notwithstanding the fact that states have so far not come to agreement on ‘which’ interpretation they should adopt. If such disagreement persists, however, it is likely that calls for new rules to break the deadlock may be put forward, in which case the third category, which is discussed below in paragraph 2.4, becomes relevant.

Apart from fundamental new characteristics of new technologies, broad formulations contained within some legal obligations might also offer the potential for states to shape the use of new technologies through interpretation. Reference here can once again be made to the use of biometrics. Under Article 27 of the fourth Geneva Convention (GC IV), for example, protected persons are entitled to ‘respect for their persons.’ This raises the question of whether, and if so, under which circumstances, states may collect and store biometric data of such persons without this breaching the obligation to ‘respect’ such persons. State practice currently suggests that this does not entail a prohibition on the gathering of such data, but more clarification may be needed.⁴²

⁴⁰ Eclectiq, “Security service of Ukraine and NATO allies potentially targeted by Russian state-sponsored threat actor.”

⁴¹ See, for example Biggio, “International Humanitarian Law and the protection of the civilian population in cyberspace: Towards a human dignity-oriented interpretation of the notion of cyber attack under Article 49 of Additional Protocol I.”

⁴² Zwanenburg, “Know thy enemy: The use of biometrics in military operations and International Humanitarian Law,” 1404-1423.

The conflict in Ukraine might speed up such developments. As the military potential of many of these new technologies is demonstrated, states would perhaps be incentivised to consider many of these interpretations and make them explicit to create clarity regarding their own legal obligations in potential future conflicts.

2.4 *New rules*

As noted, in some cases, new technology may lead states or other actors to consider that new rules are necessary. If they consider that reinterpreting existing rules is not adequate to regulate a particular technology, then this will likely lead to calls for new rules. In this case, the technology concerned falls into a third category of technologies that may require the adoption of new rules. As such, it is the fact that there is a call for new rules that determines whether a technology falls into this category and not an innate characteristic of the technology itself. It may be noted that states and other actors may not agree on the question of whether new rules are needed to regulate technology. Some may consider that existing rules are sufficient, whether or not interpreted in a particular way. This illustrates the point that there are no watertight separations between the different categories.

Numerous factors will influence whether or not states are receptive to a call for new rules. These include political, military, cultural, historical and even religious factors.⁴³ In addition, commentators have identified particular characteristics of weapons and other means of warfare that tend to make them more 'regulation-tolerant' or 'regulation-resistant'.⁴⁴ These include the effectiveness of the weapon, its novelty, its disruptiveness and its public notoriety.

Although states are still the main creators of new rules in international law, it is important to point out that non-state actors are increasingly involved in both calling for as well as developing new rules. For example, Microsoft and others have, for a number of years, been calling for a Digital Geneva Convention.⁴⁵ Such a convention would create a legally binding framework to govern states' behaviour in cyberspace in peacetime but also in armed conflict.⁴⁶

⁴³ Watts, "Regulation-tolerant weapons, regulation-resistant weapons and the law of war," 540-618.

⁴⁴ *Idem.* 618.

⁴⁵ Smith, "The need for a digital Geneva Convention."

⁴⁶ See for an appraisal of this proposal: Jetn, "The Digital Geneva Convention: A critical appraisal of Microsoft's proposal," 158.

To some commentators, the use of cyber operations in the conflict in Ukraine has further exposed the need for such a new treaty.⁴⁷ The call for such a convention does not seem to have gained much traction with states so far. However, there are examples where the efforts of civil society have played an important role in leading governments to negotiate and adopt new rules. This has been most notable in the development of treaties on anti-personnel landmines and cluster munitions.⁴⁸

Once a need for new rules has been identified, an important question to be answered is at what point in time should such new rules be developed. One potential answer to this question is to take a 'wait-and-see' approach.⁴⁹ When the characteristics and potential effects of a particular technology are not yet fully clear, states may prefer to wait to regulate such a technology until there is more clarity. They may consider that more information is needed to develop adequate regulation. They may also fear that regulation may stymie the development of technology that will be, or may turn out to be, beneficial.

Another approach is based on the 'precautionary principle,' and starts from the premise that the 'wait-and-see' approach may lead to regulation that is too little too late. It may lead to irreparable damage that could or even should have been prevented. Another risk of the 'wait-and-see' approach is that if states use new technology, they are more likely to invest in its development. As a consequence, they are then less likely to risk losing that investment by agreeing to restrictive regulation.⁵⁰ It has been submitted that if the risks of a particular technology are considered great, then the precautionary principle weighs in favour of a ban.⁵¹

An example from the conflict in Ukraine that may illustrate different points discussed above is the use of artificial intelligence (AI) in military operations, and the use of weapons employing AI in particular. On the one hand, this technology is being used in the conflict between Ukraine and Russia, making it clear that it has enormous military potential. For example, it has been reported that a Ukrainian AI company modified its commercial AI-enabled voice transcription and translation service for it to be able to process intercepted Russian communications and automatically highlight information regarding Ukrainian forces.⁵² The proven effectiveness of AI can be a reason for states to be reluctant to impose legal limitations on such use. This may explain in part why Russia has been one of the states seen as frustrating efforts to arrive at such regulation in the context of the Convention

⁴⁷ Baldassaro, "Russia-Ukraine conflict exposes need for Digital Geneva Convention."

⁴⁸ See generally Rappert, Moyes, Crowe, and Nash, "The roles of civil society in the development of standards around new weapons and other technologies of warfare," 765.

⁴⁹ Crootoof "Regulating new weapons," 21.

⁵⁰ Shereshevsky "International Humanitarian Law-making and new military technologies," 2141.

⁵¹ Crootoof "Regulating new weapons," 23.

⁵² McGee-Abe, "One year on: 10 Technologies used in the war in Ukraine."

on Certain Conventional Weapons (CCW). Talks on potentially regulating so-called Lethal Autonomous Weapon Systems (LAWS) have been formally taking place in a Group of Governmental Experts (GGE) under the auspices of the CCW since 2017. On the other hand, the actual use of AI in a conflict may also serve to underline the risks associated with the use of such technology, as well as the fact that those risks are already here. This may lead to strengthening calls for regulation. The actual use of these technologies may also contribute to bringing more clarity on what those risks are exactly, thus undercutting the argument that more time is needed to study those risks.

A final example is the use of thermobaric weapons by Russia in the Ukraine conflict.⁵³ This use has led to increased attention on these weapons. It has also occasioned some calls from within civil society to ban them.⁵⁴ States do not seem to have been receptive to these calls, however. This may be because these weapons are considered to be highly militarily effective in certain situations, particularly against concealed enemy personnel.⁵⁵ It may even be that the use of the weapon in Ukraine has served to further demonstrate this effectiveness, thereby highlighting this 'regulation-intolerant' characteristic of thermobaric weapons.

In this way, the use of technologies might highlight existing lacunae within international law, putting an emphasis on states to act and actively engage with new international legislation. The Ukraine conflict and the new uses of technologies here can, therefore, also provide a catalyst for states to further engage and consider new legal rules.

Conclusion

This chapter examined how the law can react to (the use of) new technology in armed conflict. It has drawn on the large-scale conflict in Ukraine since February 2022 for examples, which has seen the use of inter alia hypersonic missiles, biometrics, cyber operations, AI, and thermobaric weapons.

It was found that from a legal perspective, these technologies can be subdivided into three main categories. First, there are technologies that can be regulated by existing law without any problems. Second, there are technologies that raise questions concerning the applicable law, but those questions can be answered

⁵³ Rivas, Ruiz, and Umlauf, "Ukraine has accused Russia of using thermobaric weapons. Here's what makes them so devastating."

⁵⁴ Hanson, "What are thermobaric weapons? And why should they be banned?"

⁵⁵ For a discussion on the law applicable to these weapons see van Collier, "Detonating the air: The legality of the use of thermobaric weapons under International Humanitarian Law."

satisfactorily by interpreting the existing law based on accepted methods of interpretation in international law. Third and finally, existing law may not adequately address new technology even when interpreted, thus calling for new rules.

It is submitted that although these categories are useful from an analytical perspective, the lines between them are not very clear. In some cases, states or commentators may disagree on the category into which a specific (use of) technology belongs, and there may be reasonable arguments on both sides. The fact that some consider that new IHL rules are not required for cyber operations while others call for a 'digital Geneva Convention' is a case in point. Secondly, the fact that a new (use of a) technology can be adequately regulated by interpreting an existing rule does not necessarily mean that states agree on a specific interpretation. Several examples were provided in this chapter, relating inter alia to how IHL regulates cyber operations. Finally, it was found that the actual use of technology in a conflict can serve as a catalyst for thinking about how to address a specific (use of a) technology from a legal perspective. It remains to be seen what the results of this thinking will be in the case of the conflict in Ukraine.

Steven van de Put

Captain Steven van de Put is a legal advisor in the Royal Netherlands Air Force. He is currently a lecturer at the Netherlands Defence Academy, where he is responsible for teaching the military law course for the Air Force cadets. Before joining the Defence Academy he worked at several levels of command, having worked as a platoon commander and at the battalion level. He recently defended his PhD at Maastricht University, which looks at the legal accountability of UN peacekeepers for human rights violations. His main legal research interests are reparations, accountability, and international law in armed conflicts. He holds a L.L.M from Queen's University Belfast.

Marten Zwanenburg

Marten Zwanenburg is Professor of Military Law at the University of Amsterdam and at the Faculty of Military Sciences of the Netherlands Defence Academy. Previously, he held posts as legal counsel at the Ministry of Defence and subsequently at the Ministry of Foreign Affairs of the Netherlands, where he mainly advised on matters of international law regarding peace and security-related issues. Professor Zwanenburg studied international and civil law at the University of Leiden. He received his PhD from the same university in 2004. He is a member of the Editorial Boards of the Military Law

and the Law of War Review and of the Militair Rechtelijk Tijdschrift (Military Law Review, in Dutch). Professor Zwanenburg's research centres on international conflict and security law. He has published widely on peace operations, the law of armed conflict, the law of occupation, international human rights law, and international responsibility.

Bibliography

- Al Jazeera and news agencies. "What Are the Hypersonic Missiles Russia Is Using in Ukraine?" *Al-Jazeera*, 10 March 2023 <https://www.aljazeera.com/news/2023/3/10/what-are-the-hypersonic-missiles-russia-is-using-in-ukraine>.
- Arhirova, Hanna. "Minister: Ukraine will beat Russia in War of Technologies." *AP NEWS*, April 21, 2023, <https://apnews.com/article/ukraine-war-drones-technology-fe5dae6a8fabaod46fa829a549592127>.
- Baldassaro, Michael. "Russia-Ukraine Conflict Exposes Need for Digital Geneva Convention." *Carter Center*, 9 March 2022, <https://www.cartercenter.org/news/features/blogs/2022/russia-ukraine-conflict-030922.html>.
- Beecher, William. "All Sides Test Their Arms in Vietnam." *The New York Times*, September 11, 1966, <https://www.nytimes.com/1966/09/11/archives/all-sides-test-their-arms-in-vietnam.html>.
- Biggio, Giacomo. "International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I." *The Military Law and the Law of War Review* 59 (2021) 114-140.
- Brockman, Kolja, and Markus Schiller. "A Matter of Speed? Understanding Hypersonic Missile Systems." *SIPRI*, 4 February 2022, <https://www.sipri.org/commentary/topical-backgroundunder/2022/matter-speed-understanding-hypersonic-missile-systems>.
- Cassese, Antonio. "The Martens Clause: Half a Loaf or Simply Pie in the Sky?" *European Journal of International Law* 11 (2000) 187-216.
- Corn, Gary. "Cyber Operations and the Imperfect Art of 'Translating' the Law of War to New Technologies." *Articles of War*, 3 September 2020, <https://lieber.westpoint.edu/cyber-operations-imperfect-translating-law-war-new/>.
- van Collier, Arthur. "Detonating the Air: The Legality of the Use of Thermobaric Weapons under International Humanitarian Law." *International Review of the Red Cross* (Forthcoming)(2023).
- Crootof, Rebecca. "Regulating New Weapons Technology." In *The Impact of Emerging Technologies on the Law of Armed Conflict*, edited by Ronald T.P. Alcalá, Eric Talbot Jensen, 3-26. Oxford: Oxford University Press, 2019.
- Dinstein, Yoram. "Air and Missile Warfare under International Humanitarian Law." *The Military Law and Law of War Review* 52 (2013) 81-92.
- Droege, Cordula. "The Interplay between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict." *Israel Law Review* 40 (2007) 310-355.
- Ducheine, Paul, Peter Pijpers, and Kraesten Arnold. "The 'Next' War Should Have Been Fought in Cyberspace, Right? An Analysis of Cyber-Activities in the 2022 Russo-Ukraine War." Amsterdam Law School Legal Studies Research Paper No. 2022-47 (2022).

- Eclectiq. "Security Service of Ukraine and NATO Allies Potentially Targeted by Russian State-Sponsored Threat Actor." *Eclectiq* 14 February 2023, <https://blog.eclectiq.com/security-service-of-ukraine-and-nato-allies-potential-targeting-by-russian-state-sponsored-threat-actor>.
- Emtseva, Julia. "The Withdrawal Mystery Solved: How the European Court of Human Rights Decided to Move Forward with the Cases Against Russia." *EJILTALK!*, 8 February 2023, <https://www.ejiltalk.org/the-withdrawal-mystery-solved-how-the-european-court-of-human-rights-decided-to-move-forward-with-the-cases-against-russia/>.
- Federal Government of Germany, *On the Application of International Law to Cyberspace* (2021).
- Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (GC IV). 21 October 1950, 75 UNTS 975.
- Gill, Terry. "Some Thoughts on the Relationship between International Humanitarian Law and International Human Rights Law: A Plea for Mutual Respect and a Common-sense Approach." *Yearbook of International Humanitarian Law* 16 (2013) 251-266.
- Gill, Terry. "The Ius ad Bellum Anno 2040: An Essay on Possible Trends and Challenges." In *The Future Law of War*, edited by Matthew C. Waxman and Thomas W. Oakley, 25-34. Oxford: Oxford University Press, 2022.
- Graf, Jan-Phillip. "Between Accuracy and Dignity: Legal Implications of Facial Recognition for Dead Combatants." *Völkerrechtsblog*, 30 September 2022, <https://voelkerrechtsblog.org/between-accuracy-and-dignity/>.
- Hanson, Marianne. "What are Thermobaric Weapons? And Why Should They Be Banned?" *The Conversation*, 3 March 2022, <https://theconversation.com/what-are-thermobaric-weapons-and-why-should-they-be-banned-178289>.
- Human Rights Watch. "We Had No Choice: 'Filtration' and the Crime of Forcibly Transferring Ukrainian Civilians to Russia." Report 1 September 2022.
- ICJ. Legality of the Threat or Use of Nuclear Weapons, Case No. 679, Advisory Opinion, (Jul. 8, 1996).
- ICTY. Prosecutor v. Kupreskić, Case No. IT-95-16-T, Judgement, (Jan. 14, 2000).
- International Institute of Humanitarian Law. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, San Remo: International Institute of Humanitarian Law (1994).
- Ismay, Jon, Matthew Mpoke Bigg, and Andrew Kramer. "Questions Surround Russia's Use of Hypersonic Missiles in Its Latest Attack." *New York Times online*, 9 March 2023, <https://www.nytimes.com/2023/03/09/world/europe/hypersonic-missiles-russia-ukraine.html>.
- Jetn, Valentin. "The Digital Geneva Convention: A Critical Appraisal of Microsoft's Proposal." *Journal of International Humanitarian Legal Studies* 10 (2019) 158-170.
- Kalandarishvili-Mueller, Natia. "Civilians are Protected under GC IV 1949: The Illegality of Russian Filtration Camps under IHL." *EJILTALK!*, 30 November 2022, <https://www.ejiltalk.org/civilians-are-protected-under-gc-iv-1949-the-illegality-of-russian-filtration-camps-under-ihl/>.
- McGee-Abe, Jason. "One Year On: 10 Technologies used in the War in Ukraine." *Techinform*, 24 February 2023, <https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/>.
- McLaughlin, Robert, and Hitoshi Nasu. "Introduction: Conundrum of New Technologies in the Law of Armed Conflict." In *New Technologies and the Law of Armed Conflict* edited by Robert McLaughlin & Hitoshi Nasu, 1-17. New York: Springer, 2014.
- Meron, Theodor. "The Martens Clause, Principles of Humanity and the Dictates of Public Conscience." *American Journal of International Law* 94 (2000), 78-89.
- Ministry of Defence of Denmark. *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (2016).
- NATO CCDCOE. "Qualification of data as an object under IHL." *International Cyber Law toolkit*, 2023, https://cyberlaw.ccdcoe.org/wiki/Military_objectives.

- Norway. *Manual i Krigens Folkerett* (2013).
- Pomson, Ori. "Objects"? The Legal Status of Computer Data under International Humanitarian Law." *Journal of Conflict and Security Law* (forthcoming, 2023).
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). 8 June 1977, 1125 UNTS 3.
- Rappert, Brian, Richard Moyes, Anna Crowe, and Thomas Nash. "The Roles of Civil Society in the Development of Standards around New Weapons and other Technologies of Warfare." *International Review of the Red Cross* 94 (2012) 765-785.
- Reuters, "Russia Says it Repels Naval Drone Attack on Sevastopol." *Reuters*, 24 April 2023, <https://www.reuters.com/world/europe/black-sea-fleet-repels-drone-attack-sevastopol-russian-backed-governor-2023-04-24/>.
- Rivas, Ana, Roque Ruiz, and Taylor Umlauf. "Ukraine Has Accused Russia of Using Thermobaric Weapons: Here's What Makes Them So Devastating." *The Wall Street Journal*, 4 March 2022, <https://www.wsj.com/articles/ukraine-has-accused-russia-of-using-thermobaric-weapons-heres-what-makes-them-so-devastating-11646423184>.
- Royal Museums Greenwich. "Launch of Fireships Against the Spanish Armada, 7 August 1588." *Royal Museums Greenwich*, s.a. <https://www.rmg.co.uk/collections/objects/rmgc-object-11755>.
- Schondorf, Roy. "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *International Law Studies* 97 (2021) 395-406.
- Sharkov, Damien. "Russia is Using Syria to test its Next Generation of Weapons." *Newsweek*, August 24, 2017, <https://www.newsweek.com/russia-using-syria-test-next-generation-its-weapons-654689>.
- Shereshevsky, Yahli. 'International Humanitarian Law-making and New Military Technologies.' *International Review of the Red Cross* 104 (2022) 2131-2152.
- Smith, Brad. "The Need for a Digital Geneva Convention." *Microsoft*, 14 February 2017, <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.
- Tuckett, Caroline. "What's in a Name? Getting it Right for the Naval 'Drone' Attack on Sevastopol." *Articles of War*, 23 January 2023, <https://lieber.westpoint.edu/whats-in-name-getting-it-right-naval-drone-attack-on-sevastapol/>.
- Vienna Convention on the Law of Treaties (VCLT). 27 January 1980, 1155 UNTS 331.
- Watts, Sean. "Regulation-Tolerant Weapons, Regulation-Resistant Weapons and the Law of War." *International Law Studies* 91 (2015) 540-621.
- Zwanenburg, Marten. "Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law." *International Law Studies* 97 (2021) 1404-1431.
- Zwanenburg, Marten, and Steven van de Put. "The Use of Biometrics in Military Operations Abroad and the Right to Private Life." In *Towards a Data-Driven Military: A Multidisciplinary Perspective*, edited by Peter Pijpers, Mark Voskuil, Robert Beeres, 283-301. Leiden: Leiden University Press, 2023.

