# Challenging use of force, armed conflicts and the cyberspace: drones and artificial intelligence systems

## *Desafiando-se os quadros de uso da força, dos conflitos armados e do ciberespaço: drones e sistemas de inteligência artificial*

Rita Preto[*]
*Universidade Católica Portuguesa, Porto, Portugal*
*Fundação Getúlio Vargas, Rio de Janeiro – RJ, Brasil*

Beatriz Alves Serrão[*]
*Universidade Católica Portuguesa, Porto, Portugal*

## 1. Introduction

With the adoption of the Charter of the United Nations (the Charter), the most intrinsic pillar of contemporary international law[1] was improved, optimized,

[*] PhD Candidate in International Law. Joint PhD at Universidade Católica Portuguesa, Católica Porto Law School (UCP-CRP), Católica Research Centre for the Future of Law (Fundação para a Ciência e Tecnologia Scholarship, DOI 10.54499/UI/BD/152693/2022), and at Getúlio Vargas Foundation (FGV) – Rio de Janeiro Law School. LLM in European and International Law at Universidade Católica Portuguesa, Católica Porto Law School (UCP-CRP). E-mail: s-rpreto@ucp.pt.

[*] Legal Counsel at Claw Models. Fashion Law course at Milano Fashion Institute, Milan, Italy. LLM in European and International Law at Universidade Católica Portuguesa, Católica Porto Law School (UCP-CRP).

1 Over time, the norm of the prohibition of the use of force was subjected to transformational events, finally solidifying into an *opinio juris* in favor of excluding war as an attribute of the sovereignty of States. This legal obligation placed upon that States took shape in 1928, with the signing of the Kellogg-Briand Pact (Paris Peace Pact). The Pact did not accomplish everything it had set out to do, however. The concept of 'war' created a regulatory gap, with States continuing to resort to force, arguing that their warlike conduct did not meet the requirements needed to fulfill the legal threshold of war (Buchan; Tsagourias, 2021, p. 13). This issue was only improved when the UN Charter was written, which addresses the 'use of force', a much broader term than 'war'. Moreover, it institutionalized exceptions to the use of force, something that had not happened in the previous Pact. Thus, a very broad principle of prohibition was adopted in comparison with much narrower exceptions.

and institutionalized—the enshrinement in the Charter of the jus cogens norm that prohibits the use of force in international relations[2] established the "most direct measure for assuring the peace"[3]. The Security Council (SC) managed to centralize and institutionalize the collective security system—one of the exceptions to the principle of the prohibition of the use of force, along with the inherent right of individual or collective self-defense[4], which replaces the use of force as an instrument of States' foreign policy.

By voluntarily restricting the possibility of resorting to force, and with the aim of transferring this competence of reacting to internationally wrongful acts to a specific United Nations (UN) organ, the States agreed to a system that establishes not only normative, but also political and military prerequisites in order to prevent threats, acts of aggression and other acts of breach of peace, thus guaranteeing international peace and security[5].

For a considerable amount of time, the international community tried to stick to an extensive interpretation of the prohibition on the use of force along with a more or less restrictive reading of the right of self-defense, in order to avoid the distortion of the implemented international legal system[6]. However, this delicate equilibrium was fundamentally disturbed by the 9/11 attacks. Since then, the United States (US) changed their position on international relations, claiming that force can be used against the acts of non-state actors. Also, regarding the fight against terrorism, the US believes that "American state sovereignty can be combined with intervention in other states, proxy wars […] and the current drone campaign"[7].

2 "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Article 2(4), UN Charter.

3 The prevention of war and, therefore, the goal of maintaining international peace and security was the real reason the UN was established (O'connell, 2019, p. 59).

4 "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." Article 51, UN Charter.

5 "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security." Article 39, UN Charter.

6 RUYS, 2010, p. 2.

7 CHINKIN & KALDOR, 2017, p. 82.

Even though international law has attempted to keep up with those changes—albeit without losing its essence—and find the best international solutions to new challenges, such as the global war on terrorism, humanitarian crises, and cybersecurity, the upsurge of diffuse and complex threats (materialized in different forms of use of force and derived from different actors) has made it difficult for the SC to actually take up the States' role regarding the violation of Article 2(4) of the Charter. In fact, the challenges posed, particularly by terrorist organizations and cyber-attacks, have led to an increased unilateral use of force[8], which has undoubtedly been accentuated by the development of technology for military purposes.

Currently, the boots on the ground method have been relegated in the war on terrorism, in favor of using new technologies, namely drones or unmanned aerial vehicles (UAV), and fully autonomous weapons systems, which are robotic weapons imbued with artificial intelligence (AI). These can be interpreted as the third revolution in the military context, regarding their ability to select and attack targets without further human intervention after the robot is programmed for that purpose[9]. Additionally, we cannot discount cyber weapons (such as computer programs) designed with destructive capacity in mind[10].

Given their sophistication, high-precision capability (which, in turn, means less collateral damage), and the possibility of surreptitious attacks, these weapons have been the focus of great powers[11] (such as the US, Israel, Russia, France, and the UK). Their increasingly prominent presence in the international framework has raised obstacles not only in the application of jus ad bellum, but also of jus in bello, as well as in the regulation of the technology itself at an international level.

Consequently, some incidents will be analyzed throughout the article with a focus on specific issues, namely:

> (a) Some of the difficulties caused to the general prohibition on the inter-state use of force—especially in the context of the right of self-defense—by targeted killings with armed drones. Used with increasing

8 AZEREDO LOPES, 2020, p. 87.

9 SEIXAS-NUNES, 2018, p. 480.

10 O'CONNELL, 2015, p. 516.

11 Note that States also possess weapons of mass destruction (WMDs), which can be chemical, biological, or nuclear. However, these types of weapons are beyond this article's scope.

frequency to eliminate targets in third States, these attacks have generated some tension in the application of jus ad bellum and jus in bello. Thus, we will present a brief analysis of the targeted killing of Qassem Soleimani, followed by considerations about the recent targeted killing of al-Qaeda leader al-Zawahiri.
(b) From the technology perspective, some challenges posed by targeted killings fulfilled by AI-powered weapons. The concept of 'war' is changing, and autonomous weapons systems (AWS) might be a reality soon. The targeted killing of Mohsen Fakhrizadeh, carried out not by a drone, but by a weapon many call a killer robot, is an example of this emergence.
(c) Lastly, we will explore the immersion of AI systems in cyberspace and the resulting impact on one of the core principles of international humanitarian law (IHL)—the principle of distinction—since a traditional war stage no longer exists without its counterpart—cyberwar.

## 2. Unmanned Aircraft Vehicles and *Jus ad Bellum*: the assassination of Soleimani and al-Zawahiri

On January 2, 2020, former President Trump, "in a decisive defensive action to protect U.S. personnel abroad … aimed at deterring future Iranian attack plans"[12], green-lit the assassination of Qassem Soleimani, commander of the Iranian elite force IRGC, which the US had placed on the exclusion list of terrorist or terrorist-supporting organizations[13]. This attack was carried out in Iraq by the MQ-9 Reaper, which is not a fully autonomous weapon[14], as it depends on operatives for takeoff and landing, targeting infrared sensors, and, of course, for the ultimate decision to launch the missiles that fulfilled the attack.

But technological developments will not cease anytime soon. And so, by the end of that same year, tests were being developed to equip the MQ-9 Reaper with new AI technology, in order to enable it with autonomous flight, autonomous direction of its infrared sensors, and the capability to recognize objects on the ground. And they were successful[15]. Note that during this attack nine other members of the military were executed, among

12 Cf. Statement by the Department of Defense, January 2, 2020.
13 AZEREDO LOPES, 2020, p. 137.
14 Cf. p. 12.
15 HAMBLING, 2020.

them al-Muhandis, one of the main responsible parties for the coalition of pro-Iranian paramilitary groups in Iraq.

At the end of July 2022, Ayman al-Zawahiri, the second-in-command of al-Qaeda at the time of the 9/11 terrorist attacks and the new leader of al-Qaeda after Bin Laden's death, was killed by a drone strike twenty-one years later on the balcony of his home in Kabul.

In contrast to the weapon used in the first case, this attack was carried out by a drone with self-guidance capability and very specific characteristics. Instead of having an explosive warhead, this drone—in order not to cause any collateral damage, which was confirmed—included metal blades that deployed seconds before impact[16]. So, in a covert mission, without denouncing their presence and goal, the American forces eliminated the target only, due to the lack of fragmentation damage typical of conventional high-explosive missiles[17].

Faced with these examples, the role that technology plays in targeted killing missions is undeniable. On the one hand, it allows progressively more remote attacks with an increasingly powerful lethal capacity, as well as a reduction in collateral damage, and apologists of these weapons argue that only the required force is used for the mission to succeed. On the other hand, this widespread use of drones has triggered more low-intensity conflicts, making it difficult to establish a strict distinction between a peace plan and a war plan[18], and thus affecting the application of the requirements inherent to jus ad bellum and jus in bello. Hence, it is relevant to tackle some of the difficulties arising from the States' use of this type of technology: what is its legal justification?

With the advent of this technology, States initially used drones for surveillance and reconnaissance purposes. However, nowadays we encounter drones that can carry hellfire missiles much more frequently, making them better known for firing explosive weapons in targeted killings of suspected terrorists, especially in cross-border operations[19].

16 "This mission was carefully planned and rigorously minimized the risk of harm to other civilians. And one week ago, after being advised that the conditions were optimal, I gave the final approval to go get him, and the mission was a success. None of his family members were hurt, and there were no civilian casualties." Remarks by President Biden on a Successful Counterterrorism Operation in Afghanistan - The White House, August 1, 2022.

17 SCHMITT, & BIGGERSTAFF, 2022. For more information, cf. https://www.reuters.com/world/little-known-modified-hellfire-likely-killed-al-qaedas-zawahiri-2022-08-02/.

18 AZEREDO LOPES, 2020, p. 147/149.

19 CASEY-MASLEN, 2015, p. 599.

Targeted killing can be defined[20] as "the officially authorized and premeditated killing by military or intelligence official of named and identified individuals without the benefit of any judicial process,"[21] which means that this typology implies a type of actor State, a type of target, and a type of region where these actions are carried out[22].

Although the former American presidents aligned their positions regarding the existence of a transnational conflict against al-Qaeda and associated forces[23] since the attacks on New York and Washington, which justifies the application of IHL rules[24], the incidents presented lead us to a path of inapplicability of this international regime, given their circumstances. Naturally, this does not contend with the potential applicability of IHL in actual situations of armed conflict.

The US was not in an armed conflict with Iran, nor with Afghanistan following the withdrawal of the US troops[25] and, outside the framework of hostilities, we enter the context of jus ad bellum and international human rights law (IHRL). According to these, targeted killings under a drone strike are only lawful if the threat posed by the target is imminent and, and if they are the sole viable means[26], fulfilling the principle necessity.

---

20 It should be noted that there is no unambiguous definition of targeted killings under international law. For instance, the UN Special Rapporteur on Extra-Judicial, Summary or Arbitrary Executions, Philip Alston (2010), defines targeted killing as "the intentional, premeditated and deliberate use of lethal force, by States or their agents acting under colour of law, or by an organized armed group in armed conflict, against a specific individual who is not in the physical custody of the perpetrator".

21 MEISELS, & WALDRON, 2020, p. 1.

22 AZEREDO LOPES, 2020, p. 153.

23 Former President Bush started a campaign against terrorism, advocating the right of preventive self-defense via lethal force against individual targets, namely members of al-Qaeda, because the US was engaged in a transnational conflict against this organization. In the same vein, the Obama administration considered drone strikes to be legitimate because the US was engaged in an armed conflict against terrorism. Moreover, it reinforced the right to eliminate specific targets in self-defense—under conditions of imminence and necessity, and outside the framework of hostilities—if a State proved unwilling or unable to repel the threat originating in its territory (Sterio, 2012, p. 202).

24 DICKINSON, 2022.

25 "Last night in Kabul, the United States ended a 20 years of war in Afghanistan", Remarks by President Biden on the End of the War in Afghanistan - The White House, August 31, 2021.

26 According to the Article 6(1) of International Covenant on Civil and Political Rights (ICCPR), "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."

The imperative norm of the prohibition of the use of force in international relations admits some exceptions under the UN Charter, namely that the use of force is possible when the requirements of self-defense are met, or when authorized by the SC in order to reestablish international peace and security. There is also no violation of the prohibition of the use of force if a State intervenes in the territory of another State with the former's express and valid consent[27]. Now, the right of self-defense and the issue of consent have been subject to expansionist interpretations since the shift from a bilateral paradigm—State versus State—to a multilateral one—State versus non-State actors harbored in a third State—with the war on terrorism influencing the application of the existing regimes.

The examples briefly examined here present two major differences: the elimination of Soleimani marked a substantial change in US defense policy with the migration of the targeted killings technique—invoked as a means of self-defense against non-State actors—to the realm of State actors. In fact, Soleimani was part of Iran's top governing apparatus[28], regardless of whether he was unilaterally classified as a terrorist by the US.

In contrast, al-Zawahiri had been hunted since the terrorist attacks. His assassination was part of the American campaign against al-Qaeda, and therefore part of the war on terrorism, even though President Biden never used the term 'self-defense' when referring to this case. Despite the differences, these assassinations are similar on one point—in the absence of an armed conflict, it is very difficult to exclude the illegality of these uses of force by way of consent, since neither Iraq[29], nor Afghanistan[30] gave any consent, with their governments (the Taliban regime is a de facto government[31]) condemning their attacks.

27 This interpretation has been acknowledged in the International Law Association Use of Force Committee's Final Report on Aggression and the Use Force: "If consent to the deployment of military personnel is validly given, there is no use of force against the host State, and – in reference to Article 2(4) – the action is not against the "territorial integrity or political independence" of the consenting State, nor does it go against the purposes of the UN." (ILA, 2018, p. 18).

28 AZEREDO LOPES, 2020, p. 137.

29 "The incident amounts to an aggression against the State, Government and people of Iraq; ´[…] and a grave threat to the societal security of the country." Identical letters dated 6 January 2020, from the Permanent Representative of Iraq to the United Nations addressed to the Secretary-General and the President of the Security Council.

30 Taliban official Abdul Salam Hanafi stated that "All that we know is that an aerial attack has taken place here and our Islamic Emirate strongly condemns it" (Gul, 2022).

31 MARTIN, 2022, p. 5.

Regarding the killing of Soleimani, they tried to justify it under the right of self-defense, without much success. There was no armed attack from Iran and, even if the smaller scale attacks alleged by the US are added up[32], it is not lawful to invoke the right of self-defense when there is no longer an attack to repel. To this extent, the inherent requirements of armed attack followed by self-defense fail—there is, in fact, no necessity.

Nonetheless, the US has been building and defending a concept of 'naked self-defense' that "can be defined as resorting to force in self-defense, but in ways in which the means and levels of force used are not part of an armed conflict, as a matter of the technical law of war[33]". The aim is to validate targeted killings by using an armed drone, considering that the use-of-force regime is not undermined because the requirements of necessity and proportionality are met.

But this occurs at the expense of the requirement of armed attack, which is a *conditio sine qua non* of the inherent right of self-defense. In essence, this results in an argument that, outside the framework of hostilities, the regime of jus ad bellum has sufficient authority to regulate and justify operations against terrorists. In other words, the evaluation, not only of the legality of the use of force, but also of its operational execution integrates the scope of this regime.

Note that the *jus ad bellum* was not intended to be mobilized from a tactical-operational point of view, which means that this theory of self-defense provides a substitution of the necessity and proportionality requirements inherent to the institute of self-defense, by variants of these principles of IHL[34].

As we can see, we are witnessing an approximation between the concepts of targeted killings and the right of self-defense—as if it were a new type of self-defense—in a mitigation of the principle of sovereignty and an

32 "United States has undertaken certain actions in the exercise of its inherent right of self-defense. These actions were in response to an escalating series of armed attacks in recent months by the Islamic Republic of Iran and Iran-supported militias on United States forces… Over the past several months, the United States has been the target of a series of escalating threats and armed attacks by the Islamic Republic of Iran. These have included a threat to the amphibious ship USS Boxer on 18 July 2019… as well as an armed attack on 19 June 2019 by an Iranian surface-to-air missile on an unmanned United States Navy MQ-4 surveillance aircraft on a routine surveillance mission…" Letter dated 8 January 2020 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council.

33 ANDERSON, 2011, p. 8

34 CORN, 2011, p. 66.

intertwining of international legal frameworks, due to the increasing difficulty in distinguishing a peace plan from a war plan. Could a new variant of the right of self-defense be emerging?

We believe that this was an illegal invocation of the right of self-defense. There was aggression against Iran, fulfilled in the assassination of a senior Iranian official, and against Iraq[35], which had its sovereignty violated, a fact not given due importance by the US. Silence, therefore, subliminally normalized this mitigation of the principle of sovereignty, in favor of an action of 'self-defense' not against a State per se, but against targets on the territory of a State that did not consent to such intervention.

If, on the one hand, the Trump administration did not explain the attack on General Soleimani in Iraq, the same happened with the assassination of al-Zawahiri in Afghanistan, where the unwilling/unable (U/U) theory was never mentioned. Now, a missile strike from a drone that kills people within the territory of a state constitutes a use of force against that state. Therefore, a legal justification is required[36]. In the absence of a justification in the form of self-defense, as well as consent by Afghanistan, the legality of this attack could be justified in the light of the U/U theory[37], widely supported by the US.

By rectifying the absence of both substantial involvement and consent, the U/U theory emerges as a valid way to overcome the 'sovereignty barrier' to extraterritorial defensive force. Indeed, a State cannot have its sovereignty protected and, therefore, cannot invoke the prohibition on the use of force when is violating international obligations by violating the rights of other states[38]. So, States from which the non-State actors operate must

35 As put forth in Article 3(b) of the Definition of Aggression General Assembly Resolution 3314 (XXIX) of December 14, 1974, "Any of the following acts … qualify as an act of aggression: … (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State".

36 MARTIN, 2022, p. 5.

37 Under the "Unwilling and Unable" doctrine, a victim state of attacks by a non-state actor can use force in self-defense against non-state actors located in a different State (the territorial State) without that state's consent, so long as the territorial state is unwilling or unable to effectively address the threat posed by the non-state actors. For more information on the topic, cf. PETERS, & MARXSEN (eds.), Self-Defense Against Non-State Actors: Impulses from the Max Planck Trialogues on the Law of Peace and War [Max Planck Institute for Comparative Public Law & International Law (MPIL), 2017]; DEEKS, 'Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-defense' (2012), Virginia Journal of International Law.

38 AZEREDO LOPES, 2020, p. 122.

accept external intervention. This happens because it is deemed unwilling or unable to cooperate in eliminating the terrorist threat emanating from its territory—but deemed by whom? By the unilateral decision of the State that claims to have suffered a terrorist attack? These two questions highlight the reason why the underlined theory does not meet the consensus of the doctrine, and thus it would be very premature to claim that it has been consolidated as customary international law and that it could be seen as a valid justification.

Consequently, a clear tension arises between the principle of prohibition of the use of force (invoked by State A) and the principle of sovereignty and territorial integrity (inherent to State C, even if terrorist groups (B) operate from its territory). So, can a sovereign state impose its will on another sovereign state in the name of jus ad bellum and, in this sense, is the use of force through targeted killings admitted in self-defense against non-state actors on the territory of a state that has not given any prior consent? In the case at hand, it was not even questioned whether the Taliban government was unwilling or unable to face the threat posed by the leader of al-Qaeda.

The withdrawal of the American troops from Afghanistan is also coupled with the absence of a self-defense justification. This may be related to the temporal issue of this right and the fact that there was no armed attack or the imminence of one, and preemptive self-defense is not accepted in the international framework. Equally not irrelevant is the silence regarding the U/U theory, due to the international community's reluctance to accept it. Therefore, a justification for this death remains to be seen, and the reasoning that al-Zawahiri was a terrorist is not enough[39]. So, we await an explanation, and meanwhile a gap has opened at this end of the war with Afghanistan, since it was clear from Biden's speech[40] that:

the United States will rely on "over-the-horizon" capabilities to continue the war against terrorist groups in Afghanistan. Indeed, it seems the Biden administration decidedly has not declared the end of the forever war legal paradigm.[41]

39 MARTIN, 2022, p. 1/7.

40 "I made a promise to the American people that we'd continue to conduct effective counterterrorism operations in Afghanistan and beyond. We've done just that." Remarks by President Biden on a Successful Counterterrorism Operation in Afghanistan - The White House, August 1, 2022.

41 DICKINSON, 2022.

Additionally, if the US continues to claim that it is engaged in an international nonarmed conflict against terrorist groups, then it will always try to justify the use of drones to hit specific targets under IHL. Since we do not believe in the existence of an armed conflict in relation to the examples in scope, the targeted killing of al-Zawahiri was yet another precedent that may sharpen arguments in favor of using drones to carry out targeted killings under the broader applications of the right of selfdefense, such as the U/U theory. Moreover, these arguments may call into question the core exception to the use of force of the right of self-defense, extending it when the goal has always been to restrict it to cases involving armed attacks.

## 3. The age of data-driven technologies: the assassination of Mohsen Fakhrizadeh

As mentioned above, the use of drones for political-military objectives is nothing new, but their technological components are ever more advanced. UAVs can be used with great precision to eliminate individual targets, doing so with no physical risk, and avoiding collateral damage. However, their capacity to deploy lethal force is dependent on a human decision. But what about weapons with integrated AI systems? Nowadays, AI is foreshadowing a revolution in human reality.

Advances in AI technology are allowing for the future emergence of robots with computer programs enabled with decision-making capabilities, meaning they will be able to attack without additional human intervention[42]. Now, due to increasingly advanced programming capabilities, weapons with machine learning systems are being developed, which through cross-referencing data and learning from it can acquire enough knowledge to troubleshoot issues. This eliminates the need for human participation, saving resources and time.

Indeed, these systems are acquiring the ability of analyzing and interacting with their environment, identifying, and selecting targets without human intervention. Thus, we move from a paradigm of assisting in attack decisions to one where the machine makes the decision[43].

This means that the negligible time lapse underlying the learning method of machine learning systems—coupled with the increasing appeal of tech-

42 O'CONNELL, 2015, p. 526.

43 SEIXAS-NUNES, 2018, p. 484/486.

nological warfare to the detriment of conventional warfare, which demands a high human cost—will accelerate the dehumanization of armed conflict and the consequent distancing from the human conscience. An example of this dehumanization is the targeted killing of Fakhrizadeh, whose security corps were unable to react to an invisible enemy.

The assassination of Mohsen Fakhrizadeh by Israeli agents on November 27, 2020, appears to be "straight from the pages of a sci-fi novel"[44]. Comparisons with the famous Terminator movie, along with other well-known science fiction works[45] , were countless.

Responsible for the progressive development of Iran's nuclear program and unquestionable member of the Islamic Revolutionary Guard Corps—given that he occupied a prominent position in the Ministry of Defense[46]—the renowned Iranian scientist was ambushed and killed.

This was a near perfect replica of Qassem Soleimani's assassination, if not for the modus operandi employed—the drone that killed Soleimani was a method overlooked months later for Fakhrizadeh's assassination. Instead, Fakhrizadeh was killed by an AI-assisted and remotely controlled machine gun propped up on a vehicle hidden on the roadside without any personnel at the scene. The gun shot Fakhrizadeh during a car drive with his family.

This machine gun was controlled remotely via satellite by Israel's secret services. The first mandatory verification step was met in order to make it a successful attack—the absence of operatives at the site during the act[47] fulfilled the prerequisites for remote warfare (i.e., combat away from threats, without direct military confrontation). On the one hand, this bypasses financial, political, and human endeavors generally associated with war. On the other hand, it drives the increase of surreptitious and covert acts[48]. This military distancing naturally required the aforementioned AI component, which was employed to compensate for the connection's latency—it is estimated that there was a 1.6 second delay between the images broadcasting and their reception by the Israeli operative. This and the car's speed had to be considered for the weapon to be deployed successfully. In total, 15

44 MILANOVIC, 2021.

45 SHEA, 2021, p. 117.

46 Here we can also see an arbitrary deprivation of right to life under IHRL through the methodology of targeted killings.

47 BERGMAN, 2021.

48 TRENTA, 2021, p. 469.

precise shots were fired, and no collateral damage noted. His wife's life was spared[49], something that was only possible due to the facial recognition software also embedded into the weapon's AI coding.

Only a few details were published of this complex operation, based on a completely new style and method due to the chosen weapon's sophistication, which allowed the attack to be carried out in less than a minute.

In fact, it is interesting to note that, on the one hand, and unlike the drones, the weapon used reflects more traditional methods of warfare. It is possible, for example, to make an analogy with snipers: camouflaged, ideal for reconnaissance, and waiting for the right moment to carry out the mission. This human factor was replaced by a machine that, in essence, fulfilled the same purposes.

On the other hand, and in comparison to the previously mentioned drones, this slightly traditional dimension has a deeply technological counterpart. The AI system enabled a complete deterritorialization both from the ground and the air[50], allowing for completely hidden actions and plausible deniability. Now, in the age of remote-controlled warfare, time, and distance place few restrictions on killing, creating a scenario that facilitates the use of lethal force, due to the inherent dehumanization of the conflict, and that hardly meets the exceptions to the prohibition of the use of force.

### a. Stop killer robots

Although this AI-enabled weapon was not a fully autonomous weapon[51], this example made us briefly reflect on lethal autonomous weapon systems (LAWS) and the future of warfare.

As is well-known, there is still no internationally recognized, unambiguous definition of LAWS. But, in the most simplistic terms, LAWS can be understood as weapons that, through the use of state-of-the-art technology, can identify and select targets independently of human supervision or intervention (i.e., without the need for meaningful human control)[52].

49 BERGMAN, 2021.

50 Quoting the New York Times (2021), "The souped-up, remote-controlled machine gun now joins the combat drone in the arsenal of high-tech weapons for remote targeted killing. But unlike a drone, the robotic machine gun draws no attention in the sky, where a drone could be shot down, and can be situated anywhere, qualities likely to reshape the worlds of security and espionage."

51 MILANOVIC, 2021.

52 For more information, cf. ALLEN, 2022.

Even though there is no consensus on the definition of LAWS, it should be noted that the Group of Governmental Experts of the UN Convention on Certain Conventional Weapons (CCW) reiterate the need to consider the aspect of meaningful human control (MHC), which is understandable since, as it was previously mentioned, killer robots are a key source for creating asymmetries within armed conflict.

That is why the Human Rights Watch (HRW) launched the Stop Killer Robots Campaign, which calls for the total abolition of these weapons within international relations[53]. This is thus a proposed pre-emptive ban on LAWS, which is not supported by the most powerful states (i.e., USA, Israel, Russia, China). Still, it has played a crucial role in scrutinizing the obstacles that such weapons could cause in our daily lives, obviously impacting the debates held at the CCW, especially with regard to keeping MHC intact as a mandatory requirement[54].

In this sense, it is constantly reiterated that conforming to this paradigm shift automatically means conforming to the dehumanization of conflict. Weapons that can—through data processing and the pattern-crossing—draw profiles, tagging human beings according to certain stereotypes, labels, and reducing them to objects, are stripping them of their innate condition of being a person.

Naturally, this type of technology is exposed to algorithmic bias, which can make the machine create a profile that triggers and justifies the use of force[55]. And so, we reach the maximum exponent of digital dehumanization, combined with a normalization of the use of force—which has always been a measure of ultima ratio, characterized by a very broad prohibition against

53 Stop Killer Robots Campaign.

54 Quoting Peter Asaro (2012), "an international ban on autonomous weapon systems can be firmly established on the principle that the authority to decide to initiate the use of lethal force cannot be legitimately delegated to an automated process, but must remain the responsibility of a human with the duty to make a considered and informed decision before taking human lives".

55 Very recently, such a catastrophe (i.e., blindly reducing human beings to data) occurred in Kabul. On August 29th, 2021, an American drone struck terrorists who were plotting a second deadly attack that was to be carried out at Kabul International Airport. However, the victims of this attack were not, in fact, terrorists. Due to faulty information gathering that lasted eight hours, each new piece of information that was entered into the system underwent biased processing, culminating in an erroneous factual judgment. Due to the algorithmic bias affected by pre-existing prejudices, an aid worker carrying cans of water was labeled as a terrorist carrying bombs instead of water. This resulted in the deaths of ten civilians, seven children among them (Milanovic, 2021).

much narrower exceptions. Ensuring MHC is crucial in understanding how to use technology correctly and appropriately, and that the consequences of its use have implications regarding liabilities reflected in the legal context of operators[56].

To this effect, the international community has been engaged in developing and outlining a universally accepted definition of MHC. However, this has yet to be achieved[57]. What is the threshold that concretely assigns complete autonomy to an AI-powered weapon against the human operator? The exponential capacity and consequent reliance on technology has substantially changed the role of the human operator, who is unlikely to have significant control over all phases of the decision-making process in a military context.

While most States do regard the use of force as unacceptable and highly reprehensible under the terms herein, there is no consensus as to at what point in the relationship between humans and machines MHC ceases to be classified as such. Yet, several factors have been proposed as guidelines for MHC over technology. These are predictability, reliability, and transparency, as well as the guarantee that users always have accurate information and the possibility for timely intervention, so that, consequently, it is possible to establish the bond of responsibility[58].

In our point of view, regardless of the type of technology used, the self-determination capability of the operator must always be guaranteed, in that all decisions taken should derive from human consciousness, rather than from complex combinations of data that reduce the human operator to a puppet that only presses buttons because the machine says 'yes'.

It is an undeniable truth that, when it is possible to exercise MHC over weapons powered by AI systems, human operators tend to blindly trust the results achieved by technology. Nevertheless, the consciousness to deactivate a system that can achieve an unpredictable outcome should exist.[59]. AI systems tend to lack the qualities that make us irreplaceable in comparison to increasingly evolved robots—the emotions that ethical and moral judgments evoke in us.

56 Stop Killer Robots Campaign.

57 HUA, 2019, p. 131.

58 BODE & HUELSS, 2021, p. 223.

59 SEIXAS-NUNES, 2018, p. 486.

Nonetheless, this requirement must always exist, proving that ultimately, even if the system allows the selection of a target without human intervention, there is a conscious, human decision at the entering data level. Therefore, the 'self-determination decision' cannot be neglected in attempts to regulate LAWS.

In sum, driven by new algorithms and computing power, these modern AI systems will invariably impact defense institutions and leaders at their core. It is imperative that these institutions and leaders adapt and conform, given the fierce competition for digital supremacy that has already been influencing international relations and global politics. Since the greater dependency a technological system has on the use of AI, the greater its autonomy will be[60], this emerging form of AI has even been compared to the origin of the nuclear bomb[61].

Considering that several armed forces have adopted strategies and tactics designed by machines based on pattern recognition that transcend human capabilities, not only will their internal structure be affected, but also the power balance may shift. Besides, this will entail, in our view, a nearly mandatory restructuring of the concept of armed forces, in that we will be facing the replacement of human soldiers by autonomous agents[62].

Indeed, if these machines are granted capabilities and the authorization for autonomous targeting, not only will the traditional concepts of defense and deterrence be shaken[63], but the warfare paradigm will change dramatically. It should be noted, moreover, that the deep integration of robotics in various types of technology is an increasing concern in the daily lives of specialists, even if it is a conjuncture currently more present in the civilian sector than in the military domain. This is due to the possibility of self-improvement (i.e., when the program has the capability to improve itself), since it may reach a critical threshold of super-intelligence[64]—and,

60 SHEA, 2021, p. 119.

61 HUA, 2019, p. 118.

62 FOY, 2013, p. 7.

63 KISSINGER, *et. al*, 2020, p. 27.

64 See the case of Bob and Alice, for example, the AI-driven robots that Facebook engineers had to destroy because they had developed an entirely new language—one that was far from English, unintelligible to programmers and even more so to the average person. Although they did not directly contribute to this, the programmers believe that this resulted from the improvisation that the bots were supposed to perform. However, the direction taken turned out to be unexpected. A new language that facilitated communication between Bob and Alice revealed the risks that artificial intelligence could have for the future of humanity (CAETANO, 2017).

therefore, of unpredictability—meaning that AI is no longer at the service of society, but rather an existential risk for humanity[65].

## 4. The invasion of cyberspace by artificial intelligence

Regarding the future of warfare, AI has not only gained prominence in the field of LAWS, but also in the cyber domain, where cyberattacks usually occur in milliseconds, making it difficult for human operators to anticipate them. Representing a powerful mechanism in increasing the effectiveness of cyberattacks—either as a weapon or as a useful cyber-defense mechanism—deep learning[66] has greatly contributed to the propagation of actions of this magnitude by relearning and readapting itself to the underlying war framework. Nowadays, it is undeniable that cyberspace can be used for nefarious purposes that can undermine international peace and security as well as the international legal order[67].

As an example, the ongoing armed conflict in Ukraine has been a stage for cyberattacks based on AI systems. Plenty of disinformation has been spread, in the form of fake videos and audios, through bots on social media. The aim is to contradict reality and try to create a new one through this type of videos and profiles of people who do not exist. Moreover, there are phishing campaigns aimed at installing software for the purpose of stealing passwords and/or data from military personnel and diplomats[68]. And these are some of the practical results of AI systems in action.

Ergo, the use of AI in this armed conflict has so far focused on disinformation propaganda. It is through this path that one can understand the pivotal role played by AI systems in building cyberoperations, accomplished through cyberattacks that will allow the interpretation, management, and response to huge amounts of data and information. As for the mobilization of such systems within this conflict in order to interfere with the belligerents' use of LAWS, we have to refrain from comment, seeing as it is still emphasized that there is no such thing as a fully autonomous weapon yet.

65 GARCIA, 2019, p. 2

66 Subfield of machine learning that "involves the use of artificial neural networks that are inspired by the way in which neurons in the human brain are thought to interact with each other" (Seixas-Nunes, 2021, p. 434).

67 BUCHAN & TSAGOURIAS, 2021, p. 115.

68 SAMBUCCI, 2022.

Indeed, a war in today's context is and will be increasingly cybernetic. For instance, Distributed Denial-of-Service (DDoS) and Telephony Denial of Service (TDoS) are, respectively, cyberattacks intended to underload a server until it becomes unavailable to internet users (the most common), and that use the same line of attack to disrupt telephone communications in a particular area[69]. These types of attacks are relevant in warfare, in that they optimize the cyberoperations of hackers after confidential information. It was no coincidence that the Ukrainian government, at the outbreak of the conflict with the Russian Federation, started recruiting national and foreign hackers[70].

### a. The principle of distinction in warfare

If the creation of a normative legal framework or the adaptation of those already provided for LAWS has proven to be a constant challenge, the regulation of AI systems in the cyber domain is at an even earlier stage, and the required consensus for the development of a legal framework exclusively aimed at cyberwarfare has not been found at present date[71]. This does not mean, however, that this type of technology does not entail disadvantages and dangers, particularly in the IHL field, where the principle of distinction is affected by the vulnerability of erroneous recommendations or sub-optimal actions inherent to AI systems.

IHL, whose main principle is the humanization of conflict, intends to protect civilians and their property in order to minimize the former's suffering during armed conflicts. To this end, the jus in bello is based on some basic principles, including the principle of distinction. When applied to the context of cyberwar, this principle is faced with some difficulties, and is even more challenged due to the use of AI.

Now, this principle defines what are considered military objectives during an armed conflict; that is, which targets can be engaged, and which cannot

69 PRZETACZNIK, & TARPOVA, 2022, p. 3.

70 SUDERMAN & BAJAK, 2022.

71 Nonetheless, and as mentioned by Russell Buchan and Nicholas Tsagourias, "the UN General Assembly established a Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) with a view to considering whether international law in general and which international norms in particular apply to cyberspace and how they apply." (Buchan; Tsagourias, 2021, p. 115).

(civilian objectives). This distinction is crucial, since civilian objectives are entitled to immunity from direct attacks. On the other hand, they cannot 'take up arms' during a conflict, otherwise they may be prosecuted for international crimes under the Rome Statute of the International Criminal Court (ICC). This is supported by the basic rule in Article 48 of the Additional Protocol I to the Geneva Conventions (AP I)[72], and also by Article 52 of the same Protocol[73], which entitles the civilians' objects to protection (even if it is rebuttable); i.e., in gray areas where these goods are being handled for military use, there is an assumption that they remain civilian objects.

Although relatively straightforward to understand, the application of the principle of distinction to cyberwarfare is ambiguous. At the jus ad bellum level, the non-lethal nature of cyber weapons can make it difficult to assess the (i)legality of this use of force, since "there is an effects-based approach to the meaning of force in that the use of any instrument which produces death, injury or material damage and destruction can be classed as 'force' for the purposes of article 2(4)"[74]. Regarding jus in bello, and specifically the principle of distinction, differentiating civilian from military sites and equipment proves extremely complex in cyberspace[75].

The crux of the problem lies in the link between the military objective and the object that the attacker actually seeks to attack. This is where the nature of cyberspace—the multiple links between communication paths and the dependence on civilian systems, hardware, and software—takes on complexity. And it becomes even more complicated when making an analysis of the nature of the data: regardless of their nature, location, purpose, or use, can the data per se be classified as a military or civilian object?

If, during armed conflict, an attack is carried out against a computer network system of military forces, then the answer is quite clear. Conversely,

72 "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."

73 "2. Attacks shall be limited strictly to military objectives. 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 … 3. In case of doubt whether an object which is normally dedicated to civilian purposes … is being used to make an effective contribution to military action, it shall be presumed not to be so used."

74 BUCHAN & TSAGOURIAS, 2021, p. 118.

75 PASCUCCI, 2017, p. 431.

the application of this principle is called into question when an attack is directed at highly interconnected military and civilian networks. The advantages offered by cyberweapons, particularly their potential non-lethal nature, exacerbate the difficulty in applying the principle of distinction in modern warfare[76].

Moving from this more general picture to the specific conjuncture of using AI systems in cyberspace, it is evident that the obstacles deepen. Now, imagine that a State decides to delegate its national defense strategies to an AI system capable of controlling LAWS and all the means and/or machines that AI could reach through cyberspace.

At the outset, this might seem a feasible, effective, and fast solution to launch and predict cyberattacks and even traditional attacks. However, the self-learning capability and adaptability of AI systems to new software and hardware (i.e., this intrinsic ability to change and improve) invariably entails a degree of uncertainty. Why? Because the machine learning system may learn the wrong concept of attack allowed under IHL[77].

The absence of MHC, reflected in the lack of human discernment and the impossibility of repentance can culminate in:

1 – A wrong distinction between what is and what is not a legitimate military objective in cyberspace for IHL, since the principle of distinction provides, in itself, a minimum degree of human control and supervision, taking into account human judgment adapted to the particular case, something which an AI system would not be able to assess (e.g., if there were a paradigm shift and a civilian object that, until now, had a dual use ceased to apply. In essence, such technology could mistakenly learn that a civilian objective type is military, causing the destruction of such targets);

2 – A path of no return, in the sense that once an AI system is installed with the capacity to learn and act alone in an intelligent and autonomous way (i.e., without the need for human intervention), it will be practically impossible to stop certain attacks that may even be aimed at military objectives but prove to be disproportionate, or completely illegal. However, the possibility of repentance, inherent in an ethical-moral conscience, transcends such a program[78].

76 MAVROPOULOU, 2015, p. 45-51.

77 International Committee of the Red Cross, 2020, p. 467.

78 KIRK, 2019, p. 230-232.

Today, softbots[79] stand out as archetypes of AI systems deployed in the cyber environment, which operate solely and exclusively in cyberspace, possessing autonomous learning capabilities, without, however, producing violent effects. If there is no violent damage, can only military targets be affected? This is one of the many legal gaps in this cyber context, which may encourage states to purposely order attacks against civilian targets[80]— secure in the knowledge that they are doing so, but protected by the uncertainty around this legal issue that allows them not to be accused of violating IHL.

In short, after raising some relevant issues, the revolution AI has caused and will still cause becomes clear, presenting itself similarly to a black hole, in that cyberspace learning systems may never find their off button, and there are no limits to contain their scope.

## 5. Conclusion

Nowadays, we are undoubtedly witnessing a growing connection between science and warfare, something that naturally fosters instability and deepens legal insecurity due to a regulatory framework that was designed to deal with inter-state clashes involving battles between regular armed forces, the so-called "old wars"[81].

It can be said that we have entered the 'second drone era', increasingly technological and capable of quickly decimating targets (like al-Zawahiri's execution). Drones have played a key role in carrying out targeted killings. These have been justified under expansionist interpretations of the concept of self-defense that do not meet international consensus. On the other hand, the technology itself raises regulatory issues in the context of existing legal frameworks, especially with the focus on AI-powered weapons.

Fully autonomous weapons and unprecedented advances in AI—in its increased application as an indispensable component of those weapons in new contexts of war, as well as its growing role in remote warfare strategies and in deeply changing the traditional methodology of targeted killings—are not a pipe dream, but an almost tangible reality.

79 A softbot is a software agent that can analyze information in the online environment to make decisions based on a goal. The softbot is a rational agent with no hardware parts because it operates exclusively online (Kirk, 2019, p. 220).

80 KIRK, 2019, p. 230-232.

81 CHINKIN & KALDOR, 2017, p. 3.

Additionally, this technological development has had an impact on cyberspace. AI-powered weaponry mobilized in cyberspace erodes the foundations of IHL that aim to humanize conflict by protecting human values and imposing limits on warfare. This is especially true when we are faced with the possibility of carrying out attacks that, by not having devastating and destructive effects, may fall into the realm of impunity. Thus, recognizing that this is only possible due to a legal framework that has been failing to completely adapt to this type of technology is the first step to correct its many gaps.

## References

ALLEN, Gregory. DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread. *Center for Strategic & International Studies*, 2022. Obtained in: https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread.

ANDERSON, Kenneth. Targeted Killing and Drone Warfare: How We Came to Debate Whether There Is a 'Legal Geography of War'. *Future Challenges in National Security and Law*, 2011. Obtained in: http://www.futurechallengesessays.com.

ASARO, Peter. On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 2012. Obtained in: https://international-review.icrc.org/sites/default/files/irrc-886-asaro.pdf.

AZEREDO LOPES, José. Uso da Força e Direito Internacional. In: Azeredo Lopes, José (Org.), *Regimes Jurídicos Internacionais,* Vol. I. Porto: Universidade Católica Editora, 2020, 1st ed., pp. 7-212.

BERGMAN, Ronen. The Lawfare Podcast: Ronen Bergman on the A.I.-Assisted, Remote-Control Killing Machine. Lawfare Blog, 2021. Obtained in: https://www.lawfareblog.com/lawfare-podcast-ronen-bergman-ai-assisted-remote-control-killing-machine.

BODE, Ingvil & HUELSS, Hendrik. *The Future of Remote Warfare?* Artificial Intelligence Weapons Systems and Human Control. In: MCKAY, Alasdair, WATSON, Abigail., KARLSHØJ-PEDERSEN, Megan. (Org.).

*Remote Warfare*: Interdisciplinary Perspectives. Bristol: E-International Relations, 2021, pp. 218-233.

BUCHAN, Russell & TSAGOURIAS, Nicholas. *Regulating the Use of Force in International Law*: Stability and Change, 1st ed. Principles of International Law (coleção). Edward Elgar Publishing, 2021.

CAETANO, Edgar. Facebook desliga dois robôs de Inteligência Artificial que "inventaram a própria língua". *Observador*, 2017. Obtained in: https://observador.pt/2017/08/01/facebook-desliga-dois-robos-de-inteligencia-artificial-que-inventaram-a-propria-lingua/.

CASEY-MASLEN, Stuart. Pandora's Box? Drone strikes under jus ad bellum, jus in bello, and international human rights law. *International Review of the Red Cross*. Vo. 94, Issue 886, 2012. 10.1017/S1816383113000118.

CHINKIN, Christine & KALDOR, Mary. *International Law and New Wars*. Cambridge: Cambridge University Press, 2017.

CORN, Geoffrey. Self-defense Targeting: Blurring the Line between the Jus ad Bellum and the Jus in Bello. 2011. Available at SSRN: http://dx.doi.org/10.2139/ssrn.1947838.

DICKINSON, Laura. Still at War: The Forever War Legal Paradigm in Afghanistan. *Just Security*, 2022. Obtained in: https://www.justsecurity.org/81110/still-at-war-the-forever-war-legal-paradigm-in-afghanistan/.

FOY, James. Autonomous Weapons Systems: Taking the Human Out of International Humanitarian Law. *Dalhousie Journal of Legal Studies*. Vo. 23, Issue 3, 2014.

GARCIA, Eugenio. Artificial Intelligence, Peace and Security: Challenges for International Humanitarian Law. *Cadernos de Política Exterior* nº8, Instituto de Pesquisa de Relações Internacionais (IPRI), Brasília, 2019. Available at SSRN: https://ssrn.com/abstract=3595340.

GUL, Ayaz. Mum on Al-Zawahiri's Killing, Taliban Claim Renewed Resolve to Fight Terror. *Voa News*, 2022. Obtained in: https://www.voanews.com/a/taliban-reluctant-to-confirm-zawahiri-s-killing-renew-resolve-to-fight-terror-/6685733.html.

HAMBLING, David. U.S. To Equip MQ-9 Reaper Drones with Artificial Intelligence. *Forbes*, 2020. Obtained in: https://www.forbes.com/sites/davidhambling/2020/12/11/new-project-will-give-us-mq-9-reaper-drones-artificial-intelligence/?sh=4e00813d7a8e.

HUA, Shin-Shin. Machine Learning Weapons and International Humanitarian Law: Rethinking Meaningful Human Control. *Georgetown Journal of International Law*. Vo. 51, Issue 1, 2019.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Artificial intelligence and machine learning in armed conflict: A human-centred approach. *International Review of the Red Cross*. Vo. 102, Issue 913, 2020. 10.1017/S1816383120000454.

INTERNATIONAL LAW ASSOCIATION. Final Report on Aggression and the Use of Force. International Law Association, Sydney Conference, 2018.

KIRK, Aaron. Artificial Intelligence and the Fifth Domain. *Air Force Law Review*. Vo 80, 2019.

KISSINGER, Henry, SCHMIDT, Eric & HUTTENLOCHER, Daniel. *A Era da Inteligência Artificial*: e o nosso futuro humano. 3rd ed. Publicações Dom Quixote, 2021.

MARTIN, Craig. What was the International Legal Basis for the Strike on al-Zawahiri? *Just Security*, 2022. Obtained in: https://www.justsecurity.org/82605/what-was-the-international-legal-basis-for-the-strike-on-al-zawahiri/.

MAVROPOULOU, Elizabeth. Targeting in the Cyber Domain Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. *Journal of Law & Cyber Warfare*. Vo. 4, Issue 2, 2015.

MEISELS, Tamar & WALDRON, Jeremy. *Debating Targeted Killing: Counter-terrorism or Extrajudicial Execution*? 1st ed. Debating Ethics (collection). Oxford: Oxford University Press, 2020.

MILANOVIC, Marko. The Law and Tech of Two Targeted Killings. EJIL:Talk!, *Blog of the European Journal of International Law*. 2021. Obtained in: https://www.ejiltalk.org/the-law-and-tech-of-two-targeted-killings/.

O'CONNELL, Mary Ellen. *The Art of Law in the International Community*. Cambridge: Cambridge University Press, 2019.

O'CONNELL, Mary Ellen. 21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs. *Washington University Global Studies Law Review*. Vo. 13, Issue 3, 2015. Obtained in: https://scholarship.law.nd.edu/law_faculty_scholarship/1144.

PASCUCCI, Peter. Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. *Minnesota Journal of International Law*. Vo. 26, Issue 2, 2017.

PRZETACZNIK, Jakub & TARPOVA, Simona. Russia's war on Ukraine: Timeline of cyber-attacks. *European Parliamentary Research Service (EPRS)*, 2022. Obtained in: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

RUYS, Tom. *"Armed Attack" and Article 51 of the UN Charter*: Evolutions in Customary Law and Practice. Cambridge: Cambridge University Press, 2010.

SAMBUCCI, Luca. L'uso dell'intelligenza artificiale nella guerra fra Russia e Ucraina. *Notizie.AI*, 2022. Obtained in: https://www.notizie.ai/luso-dellintelligenza-artificiale-nella-guerra-fra-russia-e-ucraina/.

SCHIMTT, Michael & BIGGERSTAFF, William. The Al-Zawahiri Strike and The Law of Armed Conflict. Articles of War, *Lieber Institute West Point*, 2022. Obtained in: https://lieber.westpoint.edu/al-zawahiri-strike-law-of-armed-conflict/.

SEIXAS-NUNES, Afonso. Sistemas Autónomos de Guerra: Compatíveis com o Direito Internacional Humanitário? In: DUARTE, Maria Luísa & LANCEIRO, Rui (Org.). *O Direito Internacional e o uso da força no Século XXI*. Lisboa: AAFDL Editora, 2018, pp. 479-500.

SHEA, Annemarie. The Legal and Ethical Challenges Posed by Lethal Autonomous Weapons. *Trinity College Law Review*. Vo. 24, 2021.

STERIO, Milena. The United States' Use of Drones in the War on Terror: The (Il)legality of Targeted Killing under International Law. *Case Western Journal of International Law*. Vo. 45, Issue 5, 2012.

STONE, Mike & ALI, Idrees. Little-known modified Hellfire missiles likely killed al Qaeda's Zawahiri. *Reuters*, 2022. Obtained in: https://www.reuters.com/world/little-known-modified-hellfire-likely-killed-al-qaedas-zawahiri-2022-08-02/.

Stop Killer Robots Campaign. Obtained on September, 9, 2022, in https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/.

SUDERMAN, Alan & BAJAK, Frank. Ukrainian hackers call for volunteers before cyberwar heats up. *Associated Press*, 2022. Obtained in: https://www.csmonitor.com/World/Europe/2022/0301/Ukrainian-hackers-call-for-volunteers-before-cyberwar-heats-up

THE NEW YORK TIMES. The Scientist and the A.I.-Assisted, Remote-Control Killing Machine, 2021. Obtained in: https://www.nytimes.

com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html.

TRENTA, Luca. Remote Killing? Remoteness, Covertness, and the US Government's Involvement in Assassination. *Defence Studies*. Vo. 21, Issue 4, 2021. 10.1080/14702436.2021.1994393.

THE WHITE HOUSE. *Remarks by President Biden on a Successful Counterterrorism Operation in Afghanistan*. August 1, 2022. Obtained in: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/08/01/remarks-by-president-biden-on-a-successful-counterterrorism-operation-in-afghanistan/.

THE WHITE HOUSE. *Remarks by President Biden on the End of the War in Afghanistan*. August 31, 2021. Obtained in: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/.

Recebido em 05 de outubro de 2022.
Aprovado em 06 de março de 2024.

RESUMO: Este artigo versa sobre a utilização cada vez mais recorrente de tecnologias na prossecução de ações militares. A primeira parte foca-se na metodologia dos assassinatos seletivos, de um ponto de vista dual: num primeiro momento, com a análise das mortes de Qassem Soleimani e Ayman al-Zawahiri, destacam-se os desafios que o uso de drones para eliminar alvos em Estados terceiros colocam no quadro do jus ad bellum; num segundo momento, o foco passa a ser a tecnologia em si mesma, descrevendo-se o assassinato de Mohsen Fakhrizadeh, que foi perpetrado por uma arma imbuída por um sistema de AI que nos leva a refletir sobre o futuro da guerra moderna, e a possibilidade próxima de armas totalmente autónomas. Por fim, a segunda e última parte é direcionada para o uso da tecnologia no ciberespaço, salientando-se os obstáculos que levantam no âmbito do princípio da distinção, inerente ao regime do jus in bello. De um modo geral, a análise em causa irá assentar numa metodologia doutrinal, a qual permite refletir sobre a ordem jurídica internacional. Em concreto, partir-se-á de questões doutrinais descritivas, as quais procuram descrever e aplicar o atual estado da arte do quadro jurídico-legal internacional a casos específicos. Conclui-se, assim, que o atual quadro jurídico-legal tem de continuar a tentar adaptar-se a um novo paradigma de guerra sem, contudo, se descaracterizar.
***Palavras-chave**:* Assassinatos Seletivos; *Jus ad Bellum*; Inteligência Artificial; Sistemas de Armas Letais Autónomos; Ciberguerra; *Jus in Bello*.

ABSTRACT: This article addresses the increasingly recurrent use of technology in the pursuit of military actions. The first part focuses on the methodology of targeted killings from a dual point of view. Firstly, with the analysis of the deaths of Qassem Soleimani and Ayman al-Zawahiri, where we highlight the challenges posed by drone strikes in third States in the framework of jus ad bellum. Secondly, regarding the technology itself. We describe the assassination of Mohsen Fakhrizadeh, carried out by an AI-powered weapon, leading us to reflect on the future of warfare and fully autonomous weapons systems. Finally, the second and last part examines the use of technology in cyberspace, emphasizing the obstacles it presents under the principle of distinction, inherent in the jus in bello regime. Overall, this analysis will depend on doctrinal methods, which allow ways of thinking about the international legal system. This specifically approach will be based on descriptive research questions that seek to describe the state of the art of the current legal framework in relation to specific situations. Hence, we conclude that the current legal framework needs to find a way to adapt when faced with a new warfare paradigm, without losing its essence.
***Keywords***: Targeted Killings; *Jus ad Bellum*; Artificial Intelligence; Lethal Autonomous Weapons Systems; Cyberwarfare; *Jus in bello*.

SUGESTÃO DE CITAÇÃO: PRETO, Rita; SERRÃO, Beatriz Alves. Challenging use of force, armed conflicts and the cyberspace: drones and artificial intelligence systems. *Revista Direito, Estado e Sociedade*, Ahead of print, 2024. DOI: https://doi.org/10.17808/des.0.1855.