A Particularly Dynamic Field of International Law: Recent Developments in the Laws of Armed Conflict

Eric Tardif[*]

1 Introduction

The past decades have witnessed a considerable evolution in the field of international humanitarian law. In that sense, the last few months were particularly marked by some developments which are worthy of attention and comment: The publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* drafted by a group of experts (March 2013), coupled with the presentation of a report by another group of experts convened by the United Nations, which establishes the applicability of international law in general and the United Nations Charter in particular in cyberspace, later that year; the adoption of an Arms Trade Treaty (April 2013); and the presentation, by Amnesty International, of a report on the use of armed drones by the United States Army abroad, and the ensuing impacts on the civilian population (last October).

These developments occur in a changing landscape, marked by the evolution of geopolitics and the return to a multipolar world, the asymmetrical use of force and consequential governmental responses, the emblematic example of which is probably the United States' strategy of *signature strikes* (i.e. targeting individuals on the basis of their belonging to certain categories considered a threat to national security)[1] - which in itself constitutes an important development as it allows the possibility to plan and execute attacks from a distance. In a world where firms like Google can be treated as equals by States,

[*] LL. L. (U. Ottawa); LL. M., LL. D. (National Autonomous University of Mexico – UNAM). Doctor Tardif is a Tenured Lecturer (by Public Examination) at UNAM's Law School, in the subject of International Law.

[1] Stefan Oeter, *Methods and Means of Combat* in:, HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 115, 182 (Dieter Fleck ed., 3rd ed., 2013).

battles are no longer fought between actors of the same legal nature (i.e. State/State, company/company, etc.), and size seems to have lost its importance, as a relatively small player can take down a much bigger adversary[2], sometimes under the cover of anonymity permitted by the very nature of cyber- attacks; this is of course complicated by the fact that States, individuals and businesses alike are increasingly dependent on information and information technology: Healthcare, transportation, financial services, payroll, inventory and sales all rely on information technology in order to be efficient[3]. The foregoing poses new challenges to the laws of armed conflicts, when we compare this reality to the rules applicable to conventional or traditional warfare.

This article aims at providing an overview of the main issues related to the three major developments mentioned, in the following order: The use of armed drones (B.); the rules applicable in cyber space (C.); and the signing of the Arms Trade Treaty (D.).

2 Drones

Unmanned aerial vehicles (also known as drones because of the buzzing sound they emit, comparable to that of a male bee)[4] are used in several countries as part of a surveillance strategy, for example associated with border security or the protection of infrastructure that is deemed crucial for State interests, such as pipelines and oil refineries. Indeed, the precedents regarding the use of drones to gather intelligence during an armed conflict can be traced back to Vietnam in the 1960s; they were also used in reconnaissance missions in Bosnia and Kosovo in the 1990s[5].

It is however when they are armed that their deployment raises concern in certain circles. One of the main tasks to be performed by armed drones - and undoubtedly the most controversial one – is *targeted killings*, a concept which has not received a definition under international law as of yet[6], although it can hardly be considered a new item, as such actions have historically been carried out through sniper attacks, close range shootings,

[2] Nicolas Arpagian, *La Cyberguerre*, 4 RÉALITÉS INDUSTRIELLES 23, 24 (2010).
[3] Herbert Lin, *Cyber Conflict and International Humanitarian Law*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 515, 516 (2012).
[4] Anna Leander, *Technological Agency in the Co-Constitution of Legal Expertise and the US Drone Program*, 26 LEIDEN JOURNAL OF INTERNATIONAL LAW 811, 812 (2013).
[5] Stuart Casey-Maslen, *Pandora's Box? Drone Strikes under* Jus ad Bellum, Jus in Bello, *and International Human Rights Law*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 597, 598-599 (2012).
[6] Adam Bodnar *et al.*, *Targeted Killings (Drone Strikes) and the European Convention on Human Rights*, 32 POLISH YEARBOOK OF INTERNATIONAL LAW 189, 191 (2013).

missiles fired from ships or helicopters, explosive devices, or even poison[7]; their use is particularly associated with the United States Phoenix Program, implemented during the Vietnam era.[8]

Military attacks conducted through the use of drones can be categorized as *static* or *dynamic*: the former facet has to do with the decision to take out a specific fixed facility, and can be related to a regular bombing strategy; the latter refers to specific windows of opportunity that are identified by intelligence reports regarding the presence of a particular individual in a given location[9].

Another issue introduced by the use of targeted killings is that warfare can now be carried out from distances removed from the actual battlefield, as the decisions to execute the launching of a weapon from a drone can be taken a continent away.

2.1 The Conundrum

Drones are considered *automated* weapons, which must be distinguished from *autonomous* weapons[10], as they are still operated under human supervision and direct control, so they pose a different legal challenge than the ones found in the second category[11].

As can be expected, drone strikes are viewed with a strong negative sentiment by the general populations of most of the countries in which a survey was carried out recently,

---

[7] *Id.*, 190.

[8] Samuel Moyn, *Drones and Imagination: A Response to Paul Kahn*, 24 THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 227, 231 (2013).

[9] Samuel Issacharoff *et al.*, *Drones and the Dilemma of Modern Warfare*, NEW YORK UNIVERSITY PUBLIC LAW AND LEGAL THEORY WORKING PAPERS, Paper 404, 8 (2013);available at http://lsr.nellco.org/nyu_plltwp/404.

[10] It is important to note that fully autonomous weapons should be distinguished from those that are semi-autonomous, which are common in contemporary warfare, engaging specific targets selected by a human operator. Autonomous weapons are not necessarily unlawful, since their autonomy has no direct bearing on the probability they would cause unnecessarily suffering or superfluous injury (the prohibition of which is considered a cornerstone of modern international humanitarian law); therefore, they can be directed at combatants and military objectives. Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARVARD NATIONAL SECURITY JOURNAL FEATURES 1, 5 & 35 (2013); available at http://harvardnsj.org/2013/02/autonomous-weapon-systems-and-international-humanitarian-law-a-reply-to-the-critics/.

[11] Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 687, 690 (2012).

and some jurists have gone as far as expressing their wish to see their use banned, comparing them to landmines and cluster munitions[12]. Recently, the European Parliament has even considered the topic to be cumbersome enough to pass a resolution asking the Council to adopt a European Union common position on the use of armed drones[13].

The areas of the law involved with the study of the use of drones vary, according to the particular situation at hand: International human rights law is applicable when drones are employed outside the scope of an armed conflict; international humanitarian law, when they are deemed to be used within an armed conflict; and general international law when the attacks are viewed as violating the sovereignty of the States where they are executed[14].

As mentioned in the introduction, the ongoing debate over the use of drones was reignited by a report published by Amnesty International in October 2013 which stated that the use of these unmanned aircrafts for surveillance and targeted killings missions had caused important collateral damages in Pakistan. The Report considered the use of such weapons as one of the most controversial human rights issues in the world[15]. In it, Amnesty International asserts that the United States has launched between 330 and 374 drone strikes in Pakistan between 2004 and 2013; it is estimated that between 400 and 900 civilians have been killed, and 600 seriously injured as a result of such attacks[16].

The strategy involving the use of drones by the United States is not a recent affair, and it has been clearly documented: It is believed that in 2012 the United States Army had more than 7000 drones under its control, representing around one third of all United States military aircrafts[17], and the United States Air Force trained in 2011 more drone pilots than conventional fighter and bomber pilots[18]; also, that country's Congress has set a goal for

[12] Michael W. Lewis, *Drones and Transnational Armed Conflicts*, 3 SAINT JOHN'S JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 1, 1 (2013).
[13] Procedure 2014/2567 (RSP) of 27 February 2014; available at http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2014/2567(RSP).
[14] Leander (note 4), 818.
[15] 'Will I be next? US Drone Strikes in Pakistan', 7 (2013); available at http://www.amnesty.org/en/library/asset/ASA33/013/2013/en/041c08cb-fb54-47b3-b3fe-a72c9169e487/asa330132013en.pdf.

[16] *Id.*
[17] Casey-Maslen (note 5), 598.

the Department of Defense to replace a third of its armed air and ground combat vehicles by unmanned systems by the year 2015[19].

However, the United States are not alone in finding the use of unmanned aerial vehicles attractive: It is estimated that more than 70 States possess them[20], and among those that already have drones equipped with missiles, or that are trying to obtain them we find countries such as France, Russia, Germany, Poland, the United Kingdom, and Turkey[21]. Also, it has been documented that targeted killing missions have been executed by Israel in the occupied Palestinian territories, as well as by the United States in other countries such as Afghanistan and Yemen[22], where it is believed such strategy was first used against al Qaeda in 2002.

2.2 Arguments Tendered

The positions surrounding the use of unmanned aerial vehicles are clearly defined, and hardly reconcilable.

Supporters of drones posit that their use lowers the costs of using lethal force in at least three ways: It decreases the financial cost of employing deadly force in foreign countries, since manned aircrafts are much more expensive (the cost of an F-16 is around USD 50 million, while that of a Predator drone is about a tenth of that figure); drones reduce the political cost involved with using lethal force at the domestic level, given that sending them on a mission does not put army personnel in harm's way; finally, it reduces the accidental civilian casualties numbers due to the precision technology with which these aircrafts are equipped, so that their defenders argue that drone strikes probably kill civilians at a lower rate than other common means of warfare[23]. To strengthen their position, drone supporters emphasize the estimation that under the administration of President Obama,

---

[18] Audrey Kurth Cronin, *Why Drones Fail. When Tactics Drive Strategy*, 92 FOREIGN AFFAIRS 44, 53 (2013).
[19] Jonathan David Herbach, *Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems under the International Law of Armed Conflict*, 4(3) AMSTERDAM LAW FORUM 3, 4 (2012).
[20] Casey-Maslen (note 5), 601.
[21] Bodnar *et al*. (note 6), 191-192.
[22] *Id.*,189.
[23] Rosa Brooks, *Drones and Cognitive Dissonance*, GEORGETOWN LAW FACULTY PUBLICATIONS AND OTHER WORKS, Paper 1256, 2 & 7-8 (2013); available at http://scholarship.law.georgetown.edu/facpub/1256.

more than 3000 Al Qaeda, Taliban and other *Jihadist* operatives have been killed in Pakistan and Yemen alone[24].

However, drone strikes, whether lawful or justifiable (or not) can also increase regional instability and fuel anti-American sentiment in several parts of the world[25]. If we consider specifically the case of Al Qaeda, experts note that its propaganda has not been disrupted by drone strikes, but that on the contrary, it has been enhanced by them, allowing their use to be portrayed as indiscriminate violence against Muslim populations[26]. It can also be said that the use of drones contributes to the destruction of important evidence, as the killing of a terrorist eliminates the possibility of arresting and interrogating him to find out the future plans of the organization to which he belongs[27].

Targeted killings can be viewed as an expression of the evolution of military technology, the specific geopolitical context in which we live, and the unwillingness or inability for failed or weak States to control and eradicate the threats posed by certain groups for citizens around the world[28].

2.3 Legality under International Human Rights Law and International Humanitarian Law

As previously highlighted, unmanned aerial vehicles can be employed within the framework of an armed conflict, or outside of it. In this last case, the decision is almost never likely to be legal, if we consider the very strict rules related to the use of lethal force under international human rights law[29].

With regards to international humanitarian law, the principles of distinction and prohibition of indiscriminate attacks, the rules regarding precaution[30], as well as the more

[24] Daniel Byman, *Why Drones Work. The Case for Washington's Weapon of Choice*, 92 FOREIGN AFFAIRS 32, 33 (2013).
[25] Brooks (note 23), 10.
[26] Kurth Cronin (note 18), 46.
[27] *Id.*, 53.
[28] Issacharoff *et al.* (note 9), 8.
[29] Philip Alston, *Study on Targeted Killings*, Report to the Human Rights Council, UN Doc A/HRC/14/24/Add 6, 28 May 2010, para. 85.
[30] The principle of distinction protects civilian persons and civilian objects from the effects of military operations. It requires parties to an armed conflict to distinguish at all times, and under all circumstances, between combatants and military objectives on the one hand, and civilians and civilian objects on the other; an indiscriminate attack implies that the attacker is indifferent as to whether the targets are civilians or not, when the perpetrator fires blindly into adversarial territory without ensuring that the attacked target is of

detailed provisions covering the protection of specific objects and persons will apply to such operations, when they are carried out within the framework of an armed conflict[31].

It should be recalled here that Additional Protocol I to the Geneva Conventions establishes that while studying, developing, acquiring or adopting a new weapon, means, or methods of warfare, countries are under the obligation to determine whether its use could constitute a violation of said Protocol or any other rule of international law binding for that country[32].

Although some authors argue that the use of drones should be viewed as a symbol of mutation in the laws of war, others rather consider that they offer continuity with regards to traditional warfare[33]. The possibility to plan and execute attacks from a distance does not necessarily raise new legal issues; some experts posit that although drones represent a technological advancement, the principal issue at hand is the actual decision to use illegal force[34]. The targeted killings carried out by drones show that the use of military force in asymmetric conflicts has to be considered in a context of individuation of enemy responsibility that was so far unknown to the traditional laws of war[35]. Since the resort to targeting normally occurs in the case of members of organizations that are usually high-up in the operational structures, the identification of such individuals has to be accurate; the latter was obviously facilitated by the use of uniforms in conventional wars[36].

Another issue raised by the use of unmanned aerial vehicles is determining to what extent the international lawfulness of targeted killings should be considered under international humanitarian law or human rights law, depending on the armed conflict or law enforcement models, in the case of terrorism[37].

With regards specifically to the assertions made in the Amnesty International Report, it should be noted that most strikes are carried out in locations so remote that it is

---

military nature; All feasible precautions must be taken to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians and damage to civilian objects.

[31] William Boothby, *Some Legal Challenges Posed by Remote Attack*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 579, 582-583 (2012).

[32] Article 36 of 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, UNTS, vol. 1125, 3.

[33] Moyn (note 8), 227.

[34] Issacharoff *et al.* (note 9), 12.

[35] *Id* , 2.

[36] *Id.*, 3.

[37] Bodnar *et al.* (note 21), 191.

almost impossible for independent sources to verify what damage was indeed caused in terms of human life[38]. A related topic is of course the determination of criminal liability for possible errors committed: Should it lie with the person who identified the target as a military objective, the one authorizing the strike, or the operator of the drone, etc.?

Finally, an important concern raised by unmanned aerial vehicles is evidently their possible use, in the future, by the groups the United States and other countries are currently targeting. As controversial as the use of drones may be considered, it does not seem difficult to believe that before long such technology will fall in the hand of non-State armed groups, rendering their deployment even more difficult to regulate[39].

In the meantime, the United States has recently opened a drone base in Niger, which means that drones could potentially be used in the future in that part of the world as well[40]. This is one of more than a dozen drone bases operated by the United States outside its territory[41].

3 Cyberspace

Information and communication technologies have been found to be a useful and convenient form of waging war, which explains why they have been used in most of the conflicts since the second Iraq war[42].

In June 2013, a Group of Governmental Experts of Developments in the Field of Information and Telecommunications in the Context of International Security presented its report to the General Assembly of the United Nations[43]. In it, the Group highlights the noticeable increase in risk associated with the use of information and communication technologies, especially for criminal purposes and the conduct of disruptive activities, causing threats to individuals, business, national infrastructure and governments.[44] The 15-member group also reached a consensus affirming that international law, especially the UN

[38] Byman (note 24), 36.
[39] Casey-Maslen (note 5), 624-625.
[40] Anthony Dworkin, *Drones and Targeted Killing: Defining a European Position*, 84 EUROPEAN COUNCIL ON FOREIGN RELATIONS 1, 1 (2013).
[41] Kurth Cronin (note 18), 53.
[42] Mariarosaria Taddeo, *An Analysis for a Just Cyber Warfare*, in: 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 209, 209 (Christian Czosseck *et al.* eds,, 2012).
[43] Report of the Group of Governmental Experts of Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013).
[44] Para. 1 & 6.

Charter, applies in cyberspace; this is to be viewed as sending a strong message: States must act in cyberspace under the established international rules and principles that have guided their actions in peacetime and during conflict.

Different categories of actors intervening in cyberspace can be identified: *Classical* (the State), *mutating* (industrial groups and even smaller companies, as well as criminal groups or associations, and press groups); and *emerging* (the main industries operating in new technologies and communication fields, and individuals)[45].

The initial actions carried out in cyberspace can be traced back to 1999 when Serbian hackers attacked the internet sites of the NATO coalition as an answer to the bombardments to which they had been subjected[46]. Later, the United States Government acknowledged in 2009 that a group of activists in Iraq had been able to intercept the transmission of images generated by Predator drones thanks to low-cost software, thus disrupting a multimillion dollar military operation.[47] Likewise, it was reported that in 2011, computer experts at Nevada Air Force Base detected a virus that had infected control posts of drones operations in Afghanistan[48]. In that same year, Iran's nuclear program was the target of a sophisticated attack that sent centrifuges spinning out of control, due to a computer worm called *Stuxnet* that was probably developed by the Americans and Israelis, according to some experts; also, the populations in Burma were deprived of internet access right before the country's first national election in two decades, an act most likely coordinated by the Burmese military junta[49].

3.1 The Importance of Terminology

Several concepts can be distinguished when studying the operations carried out in cyberspace: Cyber-attack, cyber-crime and cyber-war have received different definitions. As Professor Hathaway points out, a political or national security purpose distinguishes a cyber-attack from a simple cyber-crime (internet fraud, identity theft or intellectual

[45] Lianne J. M. Boer, *Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace*, 5(3) AMSTERDAM LAW FORUM 4, 10-11 (2013).
[46] Michel Baud, *La Cyberguerre N'aura pas Lieu, Mais il Faut s'y Préparer*, 2 POLITIQUE ÉTRANGÈRE 305, 309 (2012).
[47] Arpagian (note 2), 24.
[48] Baud (note 46), 310.
[49] Oona A. Hathaway *et al*, *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 820 (2012).

property piracy); cyber-warfare must also constitute a cyber-attack, and may constitute a cyber-crime.

Baud divides computer attacks into four categories[50]: Cyber vandalism (or 'cyber *hacktivism*'), consisting in the destruction of computer data; cyber-crime and cyber-spying, which mostly target the business circles and are carried out for financial gain; and finally cyber-terrorism that looks at intimidating a government or population to call the attention on its claims, and constitutes a relatively inexpensive tool that can be used during an attack, and at the same time represents an expensive and difficult activity to protect against[51]; on a final level, we find cyber war which jeopardizes the security interests of the State.

The idea of cyber-war can also be construed in other quite different manners[52].

Another term – 'cyber operations' - can specifically be defined as operations against or via a computer or a computer system through a data stream; they can aim at infiltrating a system and collect, export, destroy, change or encrypt data, or to trigger, alter or manipulate processes controlled by the infiltrated computer system[53].

Furthermore, an additional categorization distinguishes two types of offensive operation in cyber space: Cyber-attack and cyber exploitation; the first concept refers to the use of activities meant to alter, disrupt, deceive, degrade or destroy a computer system or a network used by an adversary or the information and/or programs found in or transiting through these systems or networks; the second concept covers activities aimed at gaining access to computer systems or networks in order to obtain information found in or transiting through such systems or networks, without disturbing the normal functioning of such computer systems or networks[54].

3.2 Cyber Warfare v. Traditional Conflicts

Several aspects distinguish cyber conflicts from traditional ones. Among them, one of the most important differences regards the venue of the conflict: As opposed to a

[50] Baud (note 46), 307-308.
[51] Samuel Liles *et al.*, *Applying Traditional Military Principles to Cyber Warfare*, in: 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 169, 175 (Christian Czosseck *et al* eds,, 2012).
[52] See, for example, Karim Bouzouita, *Les Coulisses de la Révolution Tunisienne: Au Cœur de la Cyber-Guerre*, 32 GÉOSTRATÉGIQUES 145 (2011).
[53] 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', Official Working Document of the 31st International Conference of the Red Cross and Red Crescent, Doc. 31IC/11/5.1.2, 36 (2011).
[54] Lin (note 3), 518-519.

traditional conflict, where military objectives and civilian populations are often easily separable, in a cyber-conflict the space where military activity occurs is usually difficult to distinguish from the civilian one. With regards to the balance between offense and defense, in the case of a cyber-conflict the offense will always be superior to defense, since the former only needs to be successful once, while the latter must be successful every time. As far as the idea of *attribution* in concerned, it is highly difficult if not impossible to assign the responsibility of an attack to a national government in cyberspace. Also, in a cyber-conflict, non-State actors can use their information technology capabilities to achieve large scale effects that would traditionally be obtained by large scale actors. Finally, and logically, in cyber-conflicts distance has little relevance[55].

Cyber warfare can also be considered different from traditional warfare as it is not necessarily violent and destructive, and can cause severe damage to the enemy without having to display physical force or violence. Likewise, cyber warfare does not always involve human beings, since what can be construed as an action of war can be conducted by a computer virus targeting other informational infrastructures[56].

Cyber-attacks are enabled by the exposure of target systems to the rest of the world, coupled with flaws existing in such systems and that are exploited by the enemy. The direct effects of the cyber-attack are usually temporary, since the ability of the organization attacked to reprogram its system will allow it to regain control over it sooner or later. Finally it is difficult to predict the effects of the cyber-attack, as systems change constantly; what an attacker believes to have done may strongly differ from what the actual results achieved, and may also be different from what the target perceived to have happened[57].

Another key legal issues to be considered is the status of *combatant*, first addressed in the 1874 Brussels Declaration, which lists the following conditions to be considered a such: An individual must be commanded by a person responsible for his subordinates; he has to bear a fixed distinctive emblem that can be recognized at a distance, carry arms

[55] *Id*., 521.
[56] Taddeo (note 42), 211.
[57] Martin C. Libicki, *Cyberwar as a Confidence Game*, 1 STRATEGIC STUDIES QUARTERLY 132, 133-134 (2011).

openly, and carry out his operations in accordance with the laws and customs of war[58]. This of course seems difficult to achieve in cyber-space.

3.3 The Perspective of International Humanitarian Law

Some experts believe that existing *jus ad bellum* rules are not applicable in cyberspace, and that a cyber-treaty might be necessary; others, taking an approach based on analogy consider that cyber-war represents a new facet of the use of force that can be incorporated in the existing regulatory framework[59].

It is fundamental to highlight that not every cyber-attack can be considered an armed attack; there are three different schools of thought regarding this issue[60]. In the first case (*instrument-based approach*), a cyber-attack is only deemed an armed attack if it uses military weapons; the *target-based approach* considers as an armed attack a cyber-attack that targets a sufficiently important computer system; the *effects-based approach* will consider a cyber-attack as an armed attack depending on the gravity of its effects. It is therefore not totally clear what may constitute an attack, and each instance must be analyzed in accordance with the principles associated with the rules on the resort to force (*jus ad bellum*) and the ones applicable during an armed conflict (*jus in bello*)[61].

A specific issue to be addressed has to do with cyber-weapons, with regards to at least four particular legal aspects. First, it is important to point out that these can be operated by civilians; also, cyber-attacks can have consequences in the real world and not only in the virtual world, and can possibly cause loss of civilian life, injury, damage to civilian property, which means that such consequences might have to be considered under international humanitarian law; cyber weapons must be considered under the rules of *jus ad bellum*, since if it is viewed as an armed attack according to the United Nations Charter, the use of force in self-defense might be warranted; lastly the nature of a cyber-attack can

[58] Project of an International Declaration Concerning the Laws and Customs of War, 27 August 1874, Art. 9, in THE LAWS OF ARMED CONFLICTS (Dietrich Schindler & Jiri Toman eds., 1988) .
[59] Boer (note 45), 9.
[60] Hathaway (note 49), 31-33.
[61] On that topic, see Jasmine Moussa, *Can* Jus ad Bellum *Override* Jus in Bello*? Reaffirming the Separation of the Two Bodies of Law*, 90 INTERNATIONAL REVIEW OF THE RED CROSS 963 (2010).

make it difficult to determine who initiated such attack, making the subject of attribution highly relevant and difficult to assess at the same time[62].

There are two types of possible answers to cyber-attacks, one defensive and the other offensive. The first one has to do with the use of antivirus software, and the second is usually difficult to determine, since few States openly declare that they are developing such offensive capacities[63]. However, in 2012, the *United States Defense Authorization Act*[64] mentioned in its Section 954 that the Department of Defense has the capability and can be directed by the President to conduct offensive operations in cyberspace[65]. The United States also created a *cyber-command* in 2010, which can be considered a very important development as it establishes an official involvement of the Army in cyber strategy, not found for example in the case of European States[66].

3.4 The Tallinn Manual

In late 2009, the North Atlantic Treaty Organization Cooperative Cyber Defense Centre of Excellence convened an international group of approximately twenty legal scholars and practitioners, giving them the mandate to draft a manual addressing the issue of how to interpret international law in the context of cyber operations and cyber warfare. In 2013, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* was published[67].

One of the main topics addressed in the Manual has to do with how the prohibition on the use of force stated in Article 2(4) of the Charter of the United Nations applies in cyberspace; this is complicated by the fact that the mentioned provision only applies between States, and does not cover non-State actors, and the difficulty to establish what may be considered as force in cyber-space[68].

---

[62] Alan Backstrom *et al.*, *New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 483, 503-505 (2012).
[63] Baud (note 46), 312-313.
[64] 'National Defense Authorization Act for Fiscal Year 2012', Public Law 112–81, 31 December 2011.
[65] Sean Watts, *The Notion of Combatancy in Cyber Warfare*, in: 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 235, 243 (Christian Czosseck *et al.* eds,, 2012).
[66] Baud (note 46), 313-314.
[67] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, (Michael. N. Schmitt ed,, 2013).
[68] Boer (note 45), 5-9.

The Manual is structured in a way that allows consideration of the subject's following facets: States sovereignty and responsibility, use of force, law of armed conflicts in general, conduct of hostilities, the special cases involving certain persons, objects and activities, situations of occupation, and neutrality. The format of the Manual is organized in a way that black letter rules state the international law applicable to cyber warfare, followed by an extensive commentary which sets forth the rule's basis in treaty and customary law, explains how the group of experts interpreted applicable norms in the cyber context, and identifies competing positions and interpretations where a consensus among the experts could not be achieved.

The authors of the Tallinn Manual take as a starting point the opinion issued by the International Court of Justice regarding the use of nuclear weapons[69] in which it establishes that the prohibition of the use of force is applicable to any use of force, "regardless of the weapons employed"[70]. The experts also drew from the famous Nicaragua Judgment[71] as well as the Geneva and Hague Conventions, so that the majority of rules found in the Manual are usually reflected in treaties or customary international law[72]. The group of experts also highlighted the relevance of the Martens Clause for cyber warfare, which first appeared in the second Hague Convention of 1899 and was more recently incorporated in Article 1 (2) of Additional Protocol I to the Geneva Conventions, with the following wording: "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".

Although the Manual has been perceived as an important breakthrough, it has also received several criticisms which mostly focus on the fact that it leaves several aspects of the issue unresolved due to ambiguities as well as the impossibility for members of the

[69] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion), ICJ Reports 1996, 226.
[70] Boer (note 45), 10-11.
[71] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), ICJ Reports 1986, 392.
[72] Myrna Azzopardi, *The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on its Treatment of* Jus ad Bellum *Norms*, 3 ELSA MALTA LAW REVIEW 174, 175 (2013).

group of experts to reach unanimous opinions in many key subjects[73]. It has also been evidenced that the experts chosen may not portray an accurate representation of the views of all nations of the world, due to a lack of diversity of the regions of the world to which they belong[74]. Finally, it has also been asserted that the Manual does not offer a discussion of cyber operations below the threshold of an armed conflict, thus revealing the need to elaborate a list of rights and obligations of States and non-State actors in cyberspace in times of peace[75].

The reality is that the cases covered by the Tallinn Manual have hardly taken place so far in practice, and most examples cited here have occurred outside the framework of an armed conflict; for example, the operations carried out during the conflict opposing Russia and Georgia were undertaken 'in furtherance of that conflict', as stated in the Manual itself[76].

Cyber warfare has changed the traditional frames in the art of war, as the attacks are not necessarily frontal anymore, since the enemy often acts under the cover of a mask; also, States are no longer the only targets, and the private sphere can also be the object of attacks[77].

Even though the basic principles of *jus ad bellum* and *jus in bello* are applicable to cyber conflicts, their concrete implementation is at best uncertain today[78]. Some authors even consider the relevance of identifying criteria for a *just* cyber warfare[79], thus mirroring the set of rules developed centuries ago with regards to traditional war.

As stated by Professor Fiel, the developing legal framework for drones can and should guide a framework for cyber war[80].

---

[73] Oliver Kessler *et al.*, *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*, 26 LEIDEN JOURNAL OF INTERNATIONAL LAW 793, 810 (2013); *see also* Boer's article.

[74] Rain Liivoja *et al.*, *Law in the Virtual Battlespace: The Tallinn Manual and the* Jus in Bello, 15 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 45, 52 (2012).

[75] Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare. A Critical First Assessment of the New Tallinn Manual*, 18 JOURNAL OF CONFLICT & SECURITY LAW 331, 350 (2013).

[76] *Id.*, 332.

[77] Arpagian (note 2), 23.

[78] Lin (note 3), 523.

[79] *See, for example*, Taddeo (note 42), 216-217.

[80] Jessica A. Feil, *Cyberwar and Unmanned Aerial Vehicles: Using New Technologies, from Espionage to Action*, 45 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 513, 517 (2012).

4 The Arms Trade Treaty

The past few months have seen a renewed interest with regards to the issue of disarmament, especially in the case of nuclear and chemical weapons, but the most relevant development in the field has undoubtedly been the adoption of the Arms Trade Treaty.

It is estimated that between USD 45 and 60 billion worth of conventional arms sales agreements are signed each year. The main exporters are the five permanent members of the United Nations Security Council together with Germany, although some countries of the South such as Brazil and South Africa are also starting to produce and export such weapons[81]; it is considered that small arms or light weapons are manufactured in one of almost 100 States.[82] Most of the countries importing the arms are India, China, and Pakistan. Even though this area of commerce represents very important financial flows, the industry had not been regulated so far on an international basis (it is however worth mentioning that the European Union countries have been legally bound by a Code of Conduct initially drafted in1998, since 2008)[83].

According to the Stockholm International Peace Research Institute, the volume of international transfers of conventional weapons increased 17 per cent between the period of 2003-2007 and 2008-2012.[84]

The Arms Trade Treaty is not the first attempt at regulating a very lucrative industry. The most important precedent can be found in the treaty which was negotiated under the auspices of the League of Nations a century ago, the Convention for the Supervision of the International Trade in Arms and Ammunition and in Implements of War, which was opened for signature in 1925 but never entered into force[85].

---

[81] Marc Finaud, *The Arms Trade Treaty: Half Full or Half Empty?*, 6 GENEVA CENTRE FOR SECURITY POLICY 1, 1-2 (2013).

[82] Adam Arthur Biggs, *Lawmakers, Guns, & Money: How the Proposed Arms Trade Treaty can Target Armed Violence by Reducing Small Arms & Light Weapons Transfers to Non-State Groups*, 44 CREIGHTON LAW REVIEW 1311, 1320 (2011).

[83] Finaud (note 81), 2. The text of the Code of Conduct is available at http://www.consilium.europa.eu/uedocs/cmsUpload/08675r2en8.pdf.

[84] Marta Latek, *Library Briefing - The Arms Trade Treaty: Finally an Outcome and What Next?*, Library of the European Parliament, 3 (2013); available at http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130516/LDM_BRI(2013)130516_REV1_EN.pdf.

[85] Natalino Ronzitti, *Il Trattato Internazionale sul Commercio delle Armi*, 42 OSSERVATORIO DI POLITICA INTERNAZIONALE 1, 2-3 (2013).

4.1 Genesis

In Resolution 61/89 of the United Nations General Assembly adopted in 2006[86], the member States recognized that the absence of common international standards regarding the import, export, and transfer of conventional arms has contributed to conflicts, displacement of people, crime, and terrorism. This prompted the Secretary General of the Organization to establish a group of experts to examine the possibility of drafting an international instrument addressing this situation. Based on the outcome of the meetings carried out by the experts, the General Assembly adopted Resolution 64/48 in December 2009[87], calling for an international conference to be organized in 2012, to complete a draft treaty. The final project was submitted to the General Assembly in April 2013 and adopted by an overwhelming majority[88]. A geographical analysis seems to identify some kind of division between East and West, as the most reluctant States in signing the Treaty belong to the Asian and Persian Gulf regions[89].

The adoption of the final text submitted to the General Assembly was hampered by the United States presidential campaign in 2012; however, thankfully, the reluctance of that country's delegation to approve an earlier version of the treaty did not jeopardize the adoption of the final text[90]. The Treaty is the culmination of a long campaign that was initiated by a group of Nobel Peace Prize laureates and several non-governmental organizations[91]. It is also the result of what can be called 'popular diplomacy', among whose main achievements we find the signing of the Treaties on antipersonnel mines and cluster munitions[92].

4.2 Contents of the Treaty

[86] GA Res. 61/89 of 6 December 2006.
[87] GA Res. 64/48 of 2 December 2009.
[88] GA Res. 67/234 of 2 April 2013; see also *The Arms Trade Treaty (2013)*, 3 ACADEMY BRIEFING, Geneva Academy of International Humanitarian Law and Human Rights 5 (2013), available at http://www.geneva-academy.ch/docs/publications/Arms%20Trade%20Treaty%203%20WEB(2).pdf.
[89] *Le Traité sur le Commerce des Armes: Quelles Perspectives?*, Institut de Relations Internationales et Stratégiques, 3 (2013) ; available at http://www.iris-france.org/docs/kfm_docs/docs/cr-conferences/20130724-traite-commerce-armes.pdf.
[90] For a detailed account of the negotiation process of the Treaty, see Virginie Moreau, *Traité sur le Commerce des Armes: Les Négociations de la Dernière Chance ?*, NOTE D'ANALYSE DU GRIP, 1 (2012) ; available at http://www.grip.org/fr/node/716.
[91] Andrew Clapham, *The Arms Trade Treaty: A Call for an Awakening*, 2(5) EUROPEAN SOCIETY OF INTERNATIONAL LAW 1, 1 (2013).
[92] Ronzitti, (note 85), 2.

The long preamble establishes a series of principles that the States will have to follow, through an innovative technique[93]; in it, we find a reference to its notorious humanitarian component, as it specifically recognizes the problems caused to civilians by armed conflicts[94].

The first Article of the Treaty enunciates its objectives, and reads as follows:

> Article 1
> Object and Purpose
> The object of this Treaty is to:
> – Establish the highest possible common international standards for regulating or improving the regulation of the international trade in conventional arms;
> – Prevent and eradicate the illicit trade in conventional arms and prevent their diversion; For the purpose of:
> – Contributing to international and regional peace, security and stability;
> – Reducing human suffering;
> – Promoting cooperation, transparency and responsible action by States Parties in the international trade in conventional arms, thereby building confidence among States Parties.

In the following provisions, the topics covered include: The scope of the Treaty, the subject of munitions, parts and components, general implementation issues, prohibitions, export and export assessment, import, transit or trans-shipment of arms; brokering; diversion; record keeping; reporting; enforcement; international cooperation and assistance.

The heart of the Treaty is arguably found in Article 6[95], which establishes a prohibition on the transfer of arms when such transfer could go against the State's international obligations including an embargo decided by the United Nations security Council, or if the State believes that the arms transferred could be used in the commission of acts of genocide, crimes against humanity, or war crimes.

The Treaty also highlights the importance of cooperation among States in order to fulfil its proposed objectives, specifically with regards to risk mitigation, aimed at ensuring

---

[93] *Id.,* 3.

[94] Knut Doermann, *Adoption of a Global Arms Trade Treaty: Challenges Ahead*, Chatham House 1, 4 *(*2013); available at http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/160413summary.pdf.

[95] *The Arms Trade Treaty (2013)* (note 88), 23.

that the transfer does not fall within one of the prohibitions mentioned, and that it is not diverted to third countries, foreign entities, or internal actors.

One of the criticisms that have been formulated with regards to the Treaty is that it relies on an outdated categorization of weapons; Article 2 enumerates a limited list of weapons, derived from the categories covered by the United Nations Register of Conventional Arms - a voluntary international arms trade reporting system[96], but it is unclear if, for example, hand grenades or armed drones could be considered as included in the list[97].

4.3 Implementation of the Treaty

Taking into consideration the complexity of the international flows involved in the sale of arms and the existence of white, grey and black markets[98], one of the challenges of the implementation of the Arms Trade Treaty will undoubtedly be the criteria used to deny exports[99].

In that sense also, an important issue to be considered is the dependency of certain States on arms imports, many of them African, some of which are faced with the challenges brought on by weak administrative capacities and sometimes poor human rights records[100]. Article 7 mentions the 'overriding' risk that the weapons sold could be used to commit crimes, and the need for each state to determine the existence of such risk; the term suggests that the risk should be significant, but the word has been translated in Spanish to mean 'manifest', and 'significant' in Russian, so that the interpretation of such provision will probably be complicated[101]. Other ambiguities in the language used in the Treaty that can be outlined have to do for example with Article 6.3, with regards to the date to be taken into account when evaluating the possible effects of an arms sale (should it be the moment the

[96] Matthew Bolton *et al.*, *Futureproofing is Never Complete: Ensuring the Arms Trade Treaty Keeps Pace with New Weapons Technology*, 1 INTERNATIONAL COMMITTEE FOR ROBOT ARMS CONTROL 1, 3 (2013).
[97] Doermann (note 94), 4.
[98] Biggs (note 82), 1321-1326.
[99] Finaud (note 81), 4.
[100] Latek (note 84), 5.
[101] Doermann (note 94), 4.

sale is actually carried out, or possibly take into consideration a future risk?); it also seems hard to establish how the risk of corruption mentioned in Article 7 will be treated[102].

In order to be successful, the regulation of the international transfer of conventional weapons must also take into consideration the trade of components forming such weapons. Such transfers also involve the transmission of technologies and dual items (that can have both civilian and military applications)[103].

Since half of the member States of the United Nations lack a national control system of classical weapons, such mechanisms will have to be implemented and the countries will need to adopt measures criminalizing the violation of theses national standards, as well as promote international police cooperation[104]. As to the control mechanism set forth by the treaty, it is based on a reporting system: State parties will be asked to file periodic reports with the Treaty Secretariat regarding their imports and exports of armament, which will be circulated among the other member States, in a 'peer to peer' supervision scheme[105].

The role of the industry itself is also important, and the expectations of the companies involved with regards to the Treaty are that a level playing field will emerge, as for the time being only European companies are bound by the restrictive criteria of the Common Position stated in Document 2008/944[106], which deepens and widens the scope of application of the already mentioned 1998 Code of Conduct.

It can finally be noted that some States have expressed their concern that no explicit mention is made to non-State actors, but some authors consider that the Treaty also applies to such players[107].

The mere existence of the Treaty will impose a moral and political conduct to States with regards to the control over arms transfers, granting to the State parties some kind of responsible country label[108].

---

[102] *Le Traité sur le Commerce des Armes: Quelles Perspectives ?* (note 89), 7-8.
[103] Daniel Fiott *et al., The Arms Trade Treaty and the Control of Dual-Use Goods and Technologies. What Can the European Union´s Export Control Regime Offer?,* 1 INSTITUTE FOR EUROPEAN STUDIES, (2013) p. 8.
[104] *Le Traité sur le Commerce des Armes: Quelles Perspectives ?* (note 89), 9-10.
[105] Ronzitti (note 85), 5.
[106] Council Common Position 2008/944/CFSP Defining Common Rules Governing Control of Exports of Military Technology and Equipment, 13 December 2008, L 335/99; available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:EN:PDF.
[107] Ronzitti (note 85), 4.
[108] *Le Traité sur le Commerce des Armes: Quelles Perspectives?* (note 89), 7.

With regards to the possibilities of signature and ratification, in order for the Treaty to cause the desired impact, it will have to receive the backing of the main players operating on the international weapons market[109], as universality is undoubtedly one of the necessary conditions for an effective functioning of international instruments in the field of armament[110]. In that sense, it should be noted that, by April 2014, the Treaty already had been signed by more than 110 States, and over 30 had ratified it, a trend which indicates that it could enter into force by the end of the year[111].

5 Concluding Remarks

As we have seen, when new technologies are developed, they often present challenges for the application of existing bodies of law; this has also been the case for prior developments in the laws of armed conflict. The difficult legal questions arising and the differences of opinion expressed make for an uncertain future. A particular trend seems to be emerging, though, favoring the adoption of more and more autonomous robotic systems, especially due to the lack of human resources required to control the high number of already deployed systems,[112] making it possible to envisage the use of fully autonomous drones carrying out attacks based on a series of programmed vectors that would not be submitted to any human control[113], thus creating a whole new set of legal quandaries.

Scientific developments are already allowing for the creation of larger and faster unmanned aerial vehicles, and also of miniature ones, such as 'nano drones' that could be used for targeted killings possibly using poison (the so called "hummingbird drone" can fly at around 18 kilometers per hour and perch on a windowsill).[114] Also, putting aside the debate over the legality of their use, there does not seem to be, at this point, any conclusive evidence to prove that drone strikes create more enemies than they kill[115].

Generally speaking, it can also be observed that the morality and legitimacy of the practices of warfare are undergoing a profound mutation, specifically, due to the fact that

[109] *Id.*, 3.
[110] Ronzitti (note 85), 8.
[111] Article 22 establishes that the number of ratifications required for the Treaty to come into force is 50.
[112] Herbach (note 19), 19.
[113] Casey-Maslen (note 5), 624.
[114] *Id.*, 599.
[115] Kurth Cronin (note 18), 51.

the enemy is now defined in a different manner[116]. This explains in part that there seems to be some kind of a disconnect between the legal, moral and ethical considerations regarding cyber warfare[117].

As one author explains, through the use of internet, one can now even try to convince its enemy not to wage war: During the conflict opposing Russia and Georgia in 2008, 18 Georgian fighter jets were unable to take off due to a computer attack; it is highly probable that a few years earlier, these aircrafts would have been targeted in midair and possibly brought down[118].

Finally, regarding the Arms Trade Treaty, it is certainly too early to determine what its impact can have on the transfer of weapons; it seems however clear that the achievement of its objectives will as always depend on the political will of the States parties to implement its provisions, as well as the response given by the other States making up the international community.

[116] Issacharoff *et al.* (note 9), 1.
[117] Liles *et al.* (note 51), 178.
[118] Arpagian (note 2), 24.