The Rights to Privacy and Data Protection in Times of Armed Conflict

Russell Buchan and Asaf Lubin (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The Rights to Privacy and Data Protection in Times of Armed Conflict

ISBN (print): 978-9916-9565-6-4
ISBN (pdf): 978-9916-9565-7-1

2022 © NATO CCDCOE Publications
NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Cover design & content layout: Stuudio Stuudio

FOREWORD

For more than a decade, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has been analyzing cyberwar while wishing for cyber peace. That wish has been granted: what we have may be tumultuous, tense, and fragile, but it is peaceful. At least peaceful in the sense of existing below the threshold of conflict and violence. Consequently, non-war realities form the context for a vast share of our legal research. While, for instance, the first Tallinn Manual was a book about war, *Peacetime Regime for State Activities in Cyberspace* and Tallinn Manual 2.0, two later publications, sought to explore the uneasy kind of peace we are currently experiencing. This edited volume examines the rights to digital privacy and data protection in times of armed conflict while also offering a broader perspective on the fundamental differences between war- and peacetime thinking about cyber security and privacy. In doing so, it critically dissects how the rules of war and peace shape the ways our digital data is collected and utilized.

Legal writing on the relationship between international human rights law (IHRL) and international humanitarian law (IHL) has focused mainly on the rights that are closer to the kinetic theatre of war and thus also to the core of IHL. Even though the majority of States and experts take the view that both IHRL and IHL apply to cyber activities in relation to an armed conflict, the unsettled interplay between the two has rarely been elucidated further. Despite the militaries' increasing dependency on data, digital human rights are still, often reflexively, considered a peacetime legal concern. It is tacitly assumed that, should war break out, there would be more specific norms to rely on. Yet in fact, when it comes to the right to privacy, IHL is surprisingly silent. This silence cannot be deliberate, unless, of course, the laws of war were drafted by technological visionaries who foresaw the risks and opportunities that personal data could one day entail in terms of intelligence, weaponry, or human dignity. Therefore, building on the assumption that IHRL plays a key role in protecting our informational privacy before, during, and after an armed conflict, the essays in this anthology delve a great deal deeper into the realistic remits of privacy and data protection in a military context.

The editors and authors have elegantly united two clashing discourses—that of the critical necessities of conflict and that of the peace and freedom people seek in their daily lives. Naturally, implementing the ideas expressed here might create short-term practical and procedural

obstacles in planning or executing military (cyber) operations. That would call for a sobering reassessment of how much personal data is actually needed for any given military activity, be it the biometric identification of prisoners of war or protected persons, the development of AI-based cyber weapons, the preservation of evidence for postwar investigations, or the storage of records held by international criminal tribunals. Furthermore, hard questions must be asked, such as where the data comes from and whether it actually provides any national security or military advantages. But these contemplations are essential for a just and efficient military decision-making that can keep pace with its technological environment.

The discussions in the book are as relevant to the complex balancing act between civilian normality and military necessity as they are to data-processing practices within the military community. At their heart is a concern that people should be able to lead dignified lives that are not reducible to mere behavioral statistics and involve a few secrets. A study into the means to protect such lives from arbitrary violations can only advance our ability to understand both conflict and peace against their current technological backdrop and therefore makes for a truly valuable addition to CCDCOE's work.

Ann Väljataga
International law researcher
Lead of the Privacy in Conflict research project
CCDCOE

Table of Contents

DIGITAL RIGHTS IN THE *JUS POST BELLUM*

Chapter 8

The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts

Eliza Watt[1]

INTRODUCTION

The use of unmanned aerial vehicles (UAVs, or drones),[2] satellite imagery and other data collection techniques are a vital part of intelligence gathering methods used in armed conflicts.[3] Information collection facilitated

1 Dr Eliza Watt is a Lecturer in Law at Middlesex University, London, United Kingdom; a Visiting Lecturer at British Law Centre, University of Warsaw, Poland; and a guest speaker at the College of Information and Cyberspace, National Defense University, Washington D.C. USA. I wish to thank Professor Laurent Pech for his careful reviewing and commenting on this paper. Many thanks to Dr Russell Buchan and Dr Asaf Lubin for their generous guidance and feedback on the earlier drafts. I am also grateful to the participants of the 2021 NATO CCDCOE Berlin Scholars Workshop for their commentary and observations.

2 *See* Ben Knight, *Guide To Drones*, DW (June 30, 2017), https://www.dw.com/en/a-guide-to-military-drones/a-39441185.

3 Geneva Convention for Amelioration of the Conditions of the Wounded and Sick in Armed Forces in the Field; 1949 Geneva Convention for the Amelioration of the Conditions of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea; Geneva Convention Relative to the Treatment of Prisoners of War; Geneva Convention Relative to the Protection of Civilian Persons in Time of

by drones has a direct impact on a broad range of combat operations, from the ability to locate potential military objects (such as missile launchers) and mark them for destruction, in support of strategic and operational reconnaissance missions and detecting enemy movements, to supporting the safety of the ground forces through detecting surprise attacks and in identifying combatants who may be lawfully targeted.

This latter deployment of surveillance drones is particularly controversial, because the obtained data has been used for targeted killings,[4] including by armed drones.[5] The legality of such operations has been the subject of scrutiny at the United Nations (UN) and European levels and assessed chiefly in the context of international human rights law (IHRL)[6] (principally in relation to the arbitrary deprivation of life) and under the law of the use of force (*jus ad bellum*)[7] and international humanitarian law (IHL, or *jus in bello*). Nevertheless, to date little attention has been paid to States' use of UAVs for surveillance purposes and its impact on non-combatants' privacy. Yet, their constant presence causes "considerable and under-accounted-for harm to the daily lives of ordinary civilians, beyond death and physical injury",[8] terrorising men, women and children, thus giving rise to anxiety and psychological trauma among those exposed to persistent observation.

The primary legal regime that applies in situations of armed conflict is IHL. However, the relevant treaties, namely the Hague Regulations of 1899 and 1907, the Geneva Conventions I–IV of 1949 (Geneva Conventions) and their Additional Protocols of 1977 (AP I and AP II)[9] do not directly address the impact of belligerents' intelligence operations on civilians' privacy and data protection rights. Conversely, peacetime State surveillance, including mass interception and collection of foreign

War, common art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S.135 [hereinafter Common art. 2]. In the main text, referred to collectively as "Geneva Conventions".

4 For the definition of targeted killing, see Philip Alston (Special Rapporteur), *Report on Extrajudicial, Summary or Arbitrary Executions*, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) ¶ 1 [hereinafter A/HRC/14/24/Add.6].

5 *See id.*; INTERNATIONAL HUMAN RIGHTS AND CONFLICT RESOLUTION CLINIC, LIVING UNDER DRONES. DEATH, INJURY AND TRAUMA TO CIVILIANS FROM US DRONE PRACTICES IN PAKISTAN, (Stanford Law School 2012) [hereinafter LIVING UNDER DRONES].

6 *See also* Ben Emmerson (Special Rapporteur), *Report on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/HRC/25/59 (Mar. 11, 2014) [hereinafter A/HRC/25/59]; Eur. Consult. Ass., Drones and Targeted Killing: The Need to Uphold Human Rights and International Law, Doc. No. 13731 (2015), 7 ¶ 18 [hereinafter CoE Report 2015]; Christof Heyns et al., *The International Law Framework Regulating the Use of Armed Drones*, 65 INT. COMP. LAW Q. 791 (2016).

7 *See* A/HRC/14/24/Add.6, *supra* note 4; Heyns et al., *supra* note 6.

8 LIVING UNDER DRONES, *supra* note 5, ¶ vii.

9 Protocol Additional to the Geneva Conventions of 12 August, 1949, and relating to the Protection of Victims of International Armed Conflicts June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

communications, is subject to a complex set of privacy and data protection standards set out in international and regional human rights conventions, including Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR),[10] Article 8 of the European Convention on Human Rights 1950 (ECHR),[11] together with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[12]

With the advancements in drone technology and the increase in their deployment in armed conflicts, privacy concerns loom large, yet they remain unaddressed in the existing IHL framework. Consequently, this chapter asks how the right to privacy of civilians can be protected during inter-State hostilities and examines what role IHRL may have in safeguarding this right, and ultimately inquires into whether there is a need for specific regulation of intelligence gathering operations by drones.

The study begins by outlining States' use of UAVs and the impact of prolonged surveillance in war zones (Part I). Against this backdrop, Part II analyses the application of IHL and IHRL rules in such circumstances. Specifically, it identifies the interplay between these legal regimes from the perspective of intelligence gathering operations. The chapter argues that in such cases IHRL rules apply alongside IHL. Furthermore, it identifies that the principle of constant care set out in Article 57(1) of AP I to the Geneva Conventions and established under the general customary principle of precautions in attack has a significant role to play in bridging the gap left by the IHL to ensure respect of civilians' privacy and data protection rights. Part III discusses the relevance of the rules on privacy of communications to drone surveillance in armed conflict and considers when and how States are allowed to derogate from, or otherwise limit, this right. Moreover, it proposes introducing minimum data protection and privacy safeguards for drone surveillance, the latter akin to those stipulated by the European Court of Human Rights (ECtHR) for bulk collection of foreign communications.

10 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

11 European Convention for the Protection of Human Rights and Fundamental Freedoms amended by Protocols Nos 11 and 14, Nov. 4, 1950 E.T.S. 5 [hereinafter ECHR].

12 Charter of Fundamental Rights of the European Union, Oct. 2, 2000, C. 3031 [hereinafter EU Charter].

I
THE USE OF DRONES AND ITS IMPLICATIONS IN WAR ZONES AND BEYOND

A STATES' USE OF DRONES IN MILITARY OPERATIONS

Armed drones were initially operated by a handful of States, including the US, the United Kingdom (UK), Israel and Russia, in a number of combat zones, such as Afghanistan, Pakistan and Yemen, with the predominant aim of targeted killings. Recent reports attest to their increasing usage, with at least another ten States having conducted drone strikes, thirty-nine States with armed drones and twenty-nine States developing new generation armed drone technology.[13]

Drones for military use were originally designed for intelligence gathering and surveillance purposes. Equipped with high definition live-feed video, thermal infrared cameras, heat sensors, radar and mobile phone interception technology, together with such tools as licence plate readers, face recognition software and GPS trackers, UAVs allow for continuous surveillance and loitering over potential targets and/or areas and gathering of data which is then retained on military databases and shared among armed forces and intelligence agencies. With the changing nature of warfare, numerous regions across the world are seen as "battlefields" of the "global war on terror", as opposed to areas where an international armed conflict exists. Consequently, unrestricted long-term surveillance by drones is becoming commonplace.[14] Commenting on these themes on 31 August 2021[15] when marking the end of war in Afghanistan and the withdrawal of US troops, US President Joe Biden explained that the terror threat has spread beyond Afghanistan and metastasised across the world. This is one of the reasons behind US policy swaying away from the deployment of "thousands of American troops and spending billions of dollars a year in Afghanistan (to) fight a ground war",[16] and why the

13 Peter Bergen et al., *World of Drones*, NEW AMERICA (July 30, 2020), https://www.newamerica.org/international-security/reports/world-drones/.
14 CoE Report, *supra* note 6, ¶ 24 at 8.
15 *Remarks by President Biden on the End of the War in Afghanistan*, THE WHITE HOUSE (Aug. 31, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/.
16 *Id.* at 6.

President announced that US methods of engagement in future conflicts would be more remote in nature. This seems also to be the preferred policy goal of other governments and organisations, such as the European Union and the North Atlantic Treaty Organization. As drones are likely to proliferate, it becomes necessary to consider their impact on civilians, and this is addressed next.

B CIVILIAN IMPACT OF PROLONGED DRONE SURVEILLANCE AND PRIVACY IMPLICATIONS

States' UAV use has been shown to have a considerable detrimental effect beyond the death, injury and destruction immediately caused by drone strikes.[17] For example, the presence of US drones in Pakistan has reportedly caused substantial levels of fear and stress in the local population, with accounts of the experience of living under constant surveillance as harrowing.[18] Apart from common symptoms of anticipatory anxiety and post-traumatic stress disorder, persistent drone surveillance has had a negative effect on educational opportunities; on burial traditions and willingness to attend funerals; on economic, social and cultural activities; and it undermines community trust. In addition, the impact on non-combatants' privacy and data protection rights in situations of sustained drone surveillance is significant and manifold.

First, such practices are harmful, as they encroach on the respect for an individual's existence as a human being and his or her autonomy. These notions form the essence of the legal right to privacy guaranteed, *inter alia*, by Article 17(1) of the ICCPR and Article 8 of the ECHR which stipulate the right to privacy, family, home and correspondence. Second, they likely implicate the right to family life under the aforementioned provisions. Drone surveillance has been shown to impede civil liberties, including participation in social events, thus hindering familial relationships. Third, the notion of privacy also extends to the protection of individuals' homes.[19] In that sense, the "home" epitomises "a place of refuge where one can develop and enjoy domestic peace, harmony and

17 LIVING UNDER DRONES, *supra* note 5, at 73.

18 HUMAN RIGHTS CLINIC, THE CIVILIAN IMPACT OF DRONES: UNEXAMINED COSTS, UNANSWERED QUESTIONS, COLUMBIA LAW SCHOOL AND CENTRE FOR CIVILIANS IN CONFLICT (2012), 81 [hereinafter CIVILIAN IMPACT OF DRONES].

19 *See also* ICCPR, *supra* note 10, art. 17; ECHR, *supra* note 11, art. 8; U.N. Human Rights Committee, General Comment No.16: Article 17 (Right to Privacy), ¶ 5, U.N. Doc. HRI/GEN//1/Rev. 1 (Apr. 8, 1988) [hereinafter General Comment 16].

warmth without fear of disturbance".[20] Its protection relates not only to dwellings *per se*, but also covers areas over which ownership (or any other legal title) extends, including outside spaces, such as a garden.[21] It follows that every invasion of that sphere which occurs without consent of the affected individual interferes with the right to privacy.[22] Consequently, forced or clandestine trespassing, electronic surveillance practices, listening devices, covert CCTV cameras and video surveillance[23] have all been held to amount to interfering with the protected rights. Fourth, drone surveillance also instils a constant feeling of being watched which, as shown by Jeremy Bentham's Panopticon project,[24] serves as a deterrent to leading a relatively unconstrained existence. In the situation of armed conflicts, this is exacerbated as it engenders fear of a possible drone attack. Fifth, as observed by Harry Wingo, writing in the context of law enforcement agencies' use of non-lethal drones to respond to shooting accidents in the US, "surveillance drones raise privacy concerns because of their ability to harness powerful camera technology along with precision flight and pursuit capabilities that result in "drone stare"—the ability to observe persons in ways that have been previously impossible".[25] Such surveillance, especially when a drone is not visible epitomises what Michel Foucault called "the power of the gaze",[26] which creates a control mechanism by the watchers over the watched. This invariably introduces anxiety that alters how those under constant observation behave, think and interact.

Another implication of ubiquitous drone surveillance is from the perspective of data protection[27] and relates to the subsequent processing of personal information which includes images (such as those of individuals, houses, vehicles, vehicle licence plates), sound geolocation data and any other electromagnetic signals. Those subject to UAVs presence are likely to be unaware that the processing of their personal data is carried out, how such information is intended to be used and by whom. In addition, the volume of the gathered material far outpaces the operators'

20 William A. Schabas, Nowak's CCPR Commentary: U.N. International Covenant on Civil and Political Rights, 485 (N.P. Engel, 3rd ed., 2019) [hereinafter Nowak's Commentary].
21 *Id.*
22 Nowak's Commentary, *supra* note 20, at 486.
23 *See also* Peck v. United Kingdom Eur. Ct. H.R. 2003-I; Perry v. United Kingdom 39 Eur. Ct. H.R. 2003-IX.
24 *See* Jeremy Bentham, The Works of Jeremy Bentham (William Trait, 1838–43).
25 Harry Wingo, *Set Your Drones to Stun: Using Cyber Secure Quadcopters to Disrupt Active Shooters*, 17(2) Journal of Information Warfare 55, 59 (2018).
26 Michel Foucault, Discipline and Punish: The Birth of the Prison (Vintage Books 1979).
27 Privacy and data protection are related but not identical rights. Unlike privacy, data protection "regulates the processing of an individual's personal data—be it private or non-private" whereas "privacy protects an individual against intrusions in to his private sphere". Kriangsak Kittchaisaree, Public International Law in Cyberspace, 59 (Springer 2017).

capabilities to process and analyse it, thus creating an information overload, or "data crush", consequently making it almost impossible for the relevant personnel to make sense of and effectively use that information for operational purposes.[28] To help quickly turn enormous quantities of data into actionable intelligence, some military forces have utilised artificial intelligence (AI) and machine learning (ML) technologies with the assistance of private sector industries. A case in point is the US Department of Defense Project Algorithmic Warfare Cross-Functional Team (Project Maven).[29] Since 2017, its specialist algorithms that are capable of searching, identifying and categorising objects of interest within colossal volumes of material including from surveillance drones have reportedly increased efficiency and enabled decision making on the battlefield. The success of the Maven Project arguably marks the beginning of "information-age war", as the militaries are moving away from hardware-centric organisations towards being driven by AI and ML. As a result of these and similar developments, acquisition of data via drone collection is likely to increase in the future.

For at least a decade the UN,[30] a number of European institutions[31] and human rights mandate holders[32] have grappled with the issues of States' use of armed drones in conflict zones. In essence, to date these efforts have focused mainly on their deployment in extraterritorial lethal operations and the implication this has on a number of international law rules, including State sovereignty, IHL (principles of distinction, necessity and proportionality) and IHRL pertaining to the right to life. Little, or no attention has been paid to privacy and data protection of non-combatants, but there can be no doubt that these concerns call for the setting out of international normative standards due to the likely future omnipresent

28 CIVILIAN IMPACT OF DRONES, *supra* note 18, at 40.

29 Richard H. Shultz and Richard D. Clarke, *Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare*, MODERN WAR INSTITUTE (Aug. 25, 2020), https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.

30 *See also* U.N. Human Rights Council, Ensuring Use of Remotely Piloted Aircraft or Armed Drones in Counter-Terrorism and Military Operations in Accordance with International Law, Including International Human Rights Law and Humanitarian Law, (Mar. 28, 2014) U.N. Doc A/HRC/25/L.32; UN Human Rights Council, Ensuring Use of Remotely Piloted Aircraft or Armed Drones in Counter-terrorism and Military Operations in Accordance with International Law, Including International Human Rights and Humanitarian Law, (Mar. 19, 2015) UN Doc A/HRC/28/L.2.

31 *See also* Eur. Consult. Ass., Drones and Targeted Killings: the Need to Uphold Human Rights and International Law (Jan. 27, 2015); European Parliament, Written Declaration on the Use of Drones for Targeted Killings, (Jan. 16, 2012) DC\889077EN.doc; Nils Melzer, Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare (2013); EU Parliament, Resolution of 27 February 2014 on the Use of Armed Drones, (Feb. 27, 2014) 2014/2567(RSP); European Parliament, Resolution of 28 April 2016 on Attacks on Hospitals and Schools as Violations of International Humanitarian Law, (Apr. 28, 2016) (2016/2662(RSP)).

32 A/HRC/25/59, *supra* note 6.

use of drone technology. However, one question that needs to be addressed from the outset is why should this particular surveillance method be subject to specific regulation? After all, militaries have long used other long-term and pervasive techniques to gather intelligence, such as satellites. This is simply because satellite and drone technologies are different and therefore complementary, rather than rivalling each other because they are designed for different purposes. The former, being remote from the Earth's surface, provide a "macro" perspective of the given area and therefore much lower level of detail and resolution which is not useful when high accuracy is required. UAVs fill in this gap, as they operate at much lower altitudes than satellites and therefore give a "micro" view. Consequently, they are far more intrusive due to the specific and accurate information they gather and because they are easier to operate and are more manoeuvrable. This necessitates more emphasis on privacy and data protection when militaries engage in drone surveillance in and outside of combat zones as discussed below.

II
THE APPLICATION OF IHL AND IHRL TO PROLONGED DRONE SURVEILLANCE IN ARMED CONFLICT

IHL seeks to limit the effects of an armed conflict by protecting those who are not, or who are no longer, participating in the hostilities and by restricting the means and methods of warfare. IHL distinguishes between international armed conflicts (IAC) and non-international armed conflicts and this classification is crucial as different rules apply in each situation. Thus, an international armed conflict is defined in the common Article 2(1) to the Geneva Conventions as that which may "arise between two or more [States], even if the state of war is not recognized by one of them".[33] The 2016 International Committee of the Red Cross' (ICRC) revised Commentary to Geneva Convention I provides that "the determination of (IAC) existence within the meaning of Article 2(1) must be based solely on the prevailing facts demonstrating *de facto* existence

33 Common art. 2, *supra* note 3.

of hostilities between the belligerents, even without a declaration of war".[34] All four Geneva Conventions and Additional Protocol I apply to an IAC, whether or not it constitutes a declared war, regardless of parties' to the conflict recognizing it as such. Conversely, a non-international armed conflict entails a situation when the opposing parties are States and organised armed groups, or only armed groups and is subject to a more limited range of rules than those applicable to an IAC, set out in Article 3 common to the four Geneva Conventions and Additional Protocol II.

IHRL is a body of rules prescribing States' obligations to respect, protect and fulfil human rights of individuals. The high watermark in the development of this branch of international law was the adoption by the United Nations General Assembly of the Universal Declaration of Human Rights in 1948,[35] a document which for the first time in history enumerated basic civil, political, economic, social and cultural rights applicable to all. These rights were subsequently restated in, *inter alia*, the ICCPR. Generally, the rights stipulated in the human rights treaties are divided into two categories, namely absolute and qualified rights. States cannot derogate from absolute rights, such as those set out in the ICCPR, including the right to life (Article 6), the right not to be subjected to torture (Article 7) and slavery (Article 8) even in cases of emergency. By contrast, qualified rights, such as the right to privacy (Article 17), can be limited, or derogated from, as they must be balanced against public interest and can therefore be interfered with, subject to the stipulated conditions provided therein.

IHL and IHRL developed separately and differ in a number of key areas. First, IHRL predominantly applies in times of peace, whilst IHR is intended to operate during war, or an armed conflict. Second, IHRL deals with the relationship between a State and an individual. It obliges States to respect and ensure human rights to all individuals within their territory and subject to their jurisdiction.[36] In comparison, IHL aims to limit the effects of armed conflict and as such, it regulates the conduct of hostilities by State parties, recognising that when a situation of armed conflict exists between them a balance must be struck between humanity and military necessity. Finally, unlike some qualified human rights, the law of war cannot be derogated from, as it is specifically designed to

34 ICRC, Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Filed, Geneva 12 August 1946. Commentary of 2016. Article 2: Application of the Convention, https://ihl-databases.icrc.org/ihl/full/GCI-commentary.
35 Universal Declaration of Human Rights, Dec. 10, 1948, U.N.G.A. Res 217 A(III) (1948).
36 ICCPR, *supra* note 10, art. 2(1); ECHR, *supra* note 11, art. 1.

protect those who do not take part in the hostilities such as civilians, medical and religious military personnel (non-combatants), together with those who have ceased to participate in the conflict, such as wounded, shipwrecked and sick combatants and prisoners of war. This protection extends to respect for their lives, their physical and mental integrity, affords them legal guarantees and ensures that they be treated humanely in all circumstances.

Notwithstanding these differences between the two regimes, it has been recognized that there is a complementary nexus between IHL and IHRL in armed conflicts. Thus, the International Court of Justice (ICJ),[37] the Human Rights Committee (HRC), international tribunals[38] and some States[39] acknowledge that these bodies of law apply concurrently. To this end, the ICJ in the *Nuclear Weapons* Advisory Opinion[40] and in the *Wall* Advisory Opinion[41] held that the protection offered by human rights conventions, including the ICCPR, does not cease in times of war and/or armed conflict, except by operation of a derogation of the kind to be found in Article 4 of the ICCPR. In its General Comment 31, the HRC confirmed this conceptual parallel between IHL and IHRL, stating that:

> the Covenant applies also in situations of armed conflict to which the rules of international humanitarian law are applicable. While, in respect of certain Covenant rights, more specific rules of international humanitarian law may be specifically relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive.[42]

Nevertheless, it remains far from settled how these legal frameworks apply to specific situations and if any normative conflict arises between the rules in question due to their different scope and content, how it is to be resolved. International jurisprudence and academic opinion[43] offer

37 Legality of the Use or Threat of Nuclear Weapons, Advisory Opinion [1996] I.C.J Rep.226 [hereinafter Nuclear Weapons Advisory Opinion]; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion [2004] I.C.J Rep. 136 [hereinafter Wall Advisory Opinion].

38 Prosecutor v. Kunarac et al., (2001) I.C.T.Y ¶¶ 467, 471.

39 US DoD, Law of War Manual, ¶ 1.6.3.1 (2016); Germany, Federal Ministry of Defence, Law of Armed Conflict-Manual- Joint Service Regulation, ¶ 105 (2013).

40 Nuclear Weapons Advisory Opinion, *supra* note 37, ¶ 24.

41 Wall Advisory Opinion, *supra* note 37, ¶ 106.

42 U.N. Human Rights Committee, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 11, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004) [hereinafter General Comment 31].

43 *See also* Oona A. Hathaway et al., *Which Law Governs During Armed Conflict—The Relationship*

differing viewpoints. According to one approach, the IHL as *lex specialis* takes precedence over the application of the IHRL, whereas another holds that IHRL[44] complements IHL by filling its gaps, or as its interpretative tool.[45] The relationship between these two branches of law is often analyzed with reference to specific rights, such as the right to life,[46] the right to fair trial,[47] the prohibition of arbitrary detention[48] and in the context of military responses to terrorism.[49] However, perhaps one of the areas where this dichotomy is both most visible and difficult to reconcile is in the field of intelligence gathering, as it takes place in peacetime and during armed conflict alike. In the former situation, the question of which regime applies is relatively uncomplicated — these operations are mandated by both domestic statutes vesting surveillance powers to designated State organs, together with human rights law aimed at protecting individuals' privacy rights against a State's arbitrary and unlawful interference. In the context of armed conflict, the answer is more complex. This is because the law of war is the main legal framework, but as already noted, it pays little direct attention to the issue of protection of privacy. This matter is discussed next.

A INTELLIGENCE GATHERING AND PRIVACY IMPLICATIONS IN SITUATIONS OF IAC UNDER IHL

During armed hostilities, the main role of States' intelligence gathering operations is the identification of military targets. This is underpinned by the principle of distinction which is set out in Article 48 of AP I. Accordingly, to ensure respect for and protection of civilian populations and civilian objects, the parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian and

Between International Humanitarian Law and Human Rights Law, 96:6 Minn. L. Rev. 1883 (2012); William Schabas, *Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum*, 40:2 Israel L. Rev. 592 (2007).

44 Hathaway et al., *supra* note 43.

45 Nicholas Tsagourias and Alasdair Morrison, International Humanitarian Law. Cases, Materials and Commentary, 55 (Cambridge University Press 2018).

46 U.N. Human Rights Committee, Draft General Comment No. 36, Article 6: Right to Life, U.N. Doc. CCPR/C/GC/R.36/Rev (2015); U.N. Human Rights Council, *Report of the International Commission of Inquiry on Libya*, U.N. Doc. A/HRC/19/68 (2012); Al-Skeini and Others v. United Kingdom 55721/07 Eur. Ct. H.R. 2011; Case of the Santo Domingo Massacre v. Columbia 259 Inter-Am. Ct. H.R. 2012.

47 U.N. Human Right Committee, General Comment No. 32, Article 14: Right to Equality Before Courts and Tribunals and to a Fair Trial, U.N. Doc. CCPR/C/GC/32 (2007); Case of Castilla Petruzzi et al. v. Peru 52 I.A.Ct.H.R. 1999.

48 U.N. Human Rights Committee, General Comment No. 35, Article 9: Liberty and Security of Person, U.N. Doc. CCPR/C/GC/35 (2014); Hassan v. United Kingdom 29750/09 Eur. Ct. H.R. 2014.

49 Inter-American Commission on Human Rights, Report on Terrorism and Human Rights, OEA/Ser.L/V/II.116 Doc. 5 Reve. 1 corr. (2002).

military objectives and direct their operations only against the military objectives.[50]

In addition, the rule of target verification contained in Article 57(2)(a)(i) of AP I obliges those who plan or decide an attack to do "everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives".[51] To comply with these requirements, warring States are required to engage in intelligence gathering, surveillance and reconnaissance to identify the nature of the possible target to ensure that they only attack lawful military objectives.

Belligerents must also comply with the principle of proportionality[52] which prohibits attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which *would be excessive in relation to the concrete and direct military advantage anticipated*".[53] This obligation recognizes, however, collateral damage to civilians and civilian objects as part of an armed conflict. Nevertheless, those in charge of attacks must strike a balance between the military value of the destruction, neutralisation, or capture of the target and the incidental harm that the attack may cause to civilians. Intelligence gathering therefore aids the process of determination of such matters as whether there are civilians, or civilian buildings in the vicinity of the target, as well as the nature and the scale of harm likely to result from the attack.

Of equal significance in this context is also the principle of constant care stipulated in Article 57(1) of AP I, which provides that "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects".[54] Although the principle is not defined in IHL, it has been described as "the obligation of conduct, i.e. a positive and continuous obligation aimed at risk mitigation and harm prevention and the fulfilment of which requires the exercise of due diligence".[55] The rule has been referred to as a "general principle", as against one setting out specific obligations on States. That said, the use of the word "shall" in Article 57(1) is legally binding on the parties to AP I and as a consequence it applies to all domains of warfare and all levels

50 AP I, *supra* note 9, art. 48.
51 *Id.* art. 57(2)(a)(i).
52 *Id.* arts. 51(5)(b), 57(2)(a)(ii) and 57(2)(b).
53 *Id.* art. 51(5)(b) (emphasis added).
54 *Id.* art. 57(1).
55 International Law Association Study Group on the Conduct of Hostilities in the 21st Century, The Conduct of Hostilities and International Humanitarian Law. Challenges of 21st Century Warfare. 93 INT'L. L. Stud.322 (2017) [hereinafter ILA Study Group].

of operations.[56] However, since the title to Article 57 refers to "precautions in attack", this provision is often read as applying only in situations of attacks (i.e. "acts of violence against the adversary, whether in offence or in defence")[57] and therefore in conjunction with the scenarios enumerated in Article 57(2)–(5). This view seems quite limited though, as it has been advanced that the obligation to take constant care to spare civilian population must necessarily apply to the entire range of military operations, not only to attacks.[58] This broader reading is preferable because on the more restrictive interpretation, Article 57 would only pertain to attacks and specific situations set out in sub-paragraphs 2–5,[59] thus discounting a whole spectrum of military activities. Of note in this context is the ICRC Commentary on AP I (ICRC Commentary) which interprets "military activities" for the purposes of Article 57 as a term which "shall be understood to mean any movements, manoeuvres and *other activities whatsoever carried out by the armed forces with the view to combat*".[60] The doctrine of constant care must therefore be construed as a "stand-alone" obligation, that is, in addition to the general rules of taking precautionary measures in attacks contained in Article 57(2)–(5).[61] Some States, such as the UK, support such an expansive interpretation of this provision. Thus, the UK Manual of the Law of Armed Conflict[62] considers "military operations" to be a wider term than "attack", as they include the movement and deployment of armed forces.[63] The document further asserts that "the commander will have to bear in mind the effect on the civilian population of what he is planning to do and take steps to reduce that effect as much as possible. In planning or deciding on, or carrying out attacks, however, those responsible have more specific duties."[64] Therefore, based on the premise that the duty of constant care applies throughout the entire spectrum of combat operations, the next section examines whether it can serve to close the normative gap in the IHL framework by placing privacy and data protection obligations on States' intelligence operations.

56 *Id.* at 43.
57 AP I, *supra* note 9, art. 49(1).
58 ILA Study Group, *supra* note 55, at 42.
59 AP I, *supra* note 9, art. 57(2)–(5).
60 ICRC, 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. Commentary of 1987. Precautions in Attack, ¶ 2191 (1987) (emphasis added).
61 ILA Study Group, *supra* note 55, at 43.
62 UK MoD, The Manual of the Law of Armed Conflict (Oxford University Press 2003).
63 *Id.* footnote 187 to ¶ 5.32.
64 *Id.* ¶ 5.32.1.

B INTELLIGENCE GATHERING AND PRIVACY IMPLICATIONS IN SITUATIONS OF IAC UNDER IHRL

International treaties, including the ICCPR and the ECHR, place an obligation on each State party to respect and ensure to all individuals the rights recognized in these instruments, including the right to privacy contained in Article 17 and Article 8 respectively. As drone surveillance is often conducted extraterritorially, the question that arises is whether States are bound by their treaty obligations in such instances. The matter of extraterritorial application of human rights treaties is not entirely settled, but as a general rule States owe human rights obligations predominantly to those who are within their territory. However, when a State exercises effective control over foreign area (the spatial model),[65] or physical control over an individual in a foreign country (the personal model),[66] then the human rights duties will extend beyond its borders.

As a general rule, States must adopt legislative or other measures to give effect to the rights stipulated in the treaties and provide effective domestic remedies for their violation. However, these requirements are subject to two caveats. First, States may derogate from their treaty obligations by temporarily suspending certain rights during public emergencies. Second, they may limit non-absolute rights and freedoms on the basis of permissible limitations clauses. The next part discusses both these mechanisms in the context of the right to privacy.

1 *Derogations*

According to Article 4(1) of the ICCPR in times of officially proclaimed public emergency which threatens the life of the nation, a State party to the Covenant may derogate from some of its obligations[67] which includes Article 17.[68] States can do so by adopting derogating measures, but these must be of an exceptional and temporary nature. Moreover, prior to a State invoking Article 4 a number of conditions must be met.[69] First, the situation has to amount to a public emergency, which threatens the life of the nation.[70] Although not every disturbance or catastrophe qualifies

65 Wall Advisory Opinion, *supra* note 37, ¶¶ 107–13.
66 General Comment 31, *supra* note 42, ¶ 10; *Al-Skeini*, *supra* note 46, ¶ 131.
67 ICCPR, *supra* note 10, art. 4(1).
68 *Id.* art. 4(1). However, art 4(2) lists a number of non-derogable rights.
69 *See* U.N. Human Rights Committee, CCPR General Comment No 29: Article 4: Derogations During A State of Emergency, U.N. Doc. CCPR/C/21/Rev.1/Add.11. (Aug. 31, 2001) [hereinafter General Comment 29].
70 ICCPR, *supra* note 10, art. 4(1).

as a public emergency, an international armed conflict falls within the meaning of "public emergency" stipulated in Article 4(1) and consequently gives States the right to derogate from certain human rights.[71] Secondly, a relevant government organ must officially proclaim a state of emergency.[72] Such prior pronouncement is a technical pre-requisite for the application of Article 4, as without it any derogation from the Covenant's rights will constitute a violation of international law.[73] Further, the language of Article 4(1) makes an explicit reference to the principle of proportionality, stating that the Covenant rights may be derogated from only "to the extent strictly required by the exigencies of the situation".[74] This provision represents the most important limitation on permissible derogation measures and requires that "the degree of interference and the scope of the measure must stand in a reasonable relation to what is actually necessary to combat an emergency threatening the life of the nation".[75] Whether or not States comply with the principle of proportionality when taking measures to derogate is subject to review by the HRC.[76] In addition, Article 4(3) requires State parties to immediately inform the other State parties through the UN Secretary-General of the provision(s) it has derogated from and the reasons for such measures.[77] The duty of notification is essential, as not only does it enable the HRC to discharge its functions when assessing whether the measures taken by the State were strictly required by the exigencies of the situation, but it also permits other State parties to monitor compliance with the provisions of the Covenant.[78] Thus far, there appears to be not a single country that has taken measures to derogate from Article 17 specifically on the grounds of the existence of, or the involvement in an armed conflict.

Unlike Article 4 of the ICCPR, Article 15 of the ECHR allows States to derogate from their Convention obligations not only "during public emergencies threatening the life of the nation", but also in the time of war.[79] However, as in the case of Article 4 of the ICCPR by virtue of Article 15(2) of the ECHR, States may derogate from Article 8, but must meet both

71 General Comment 29, *supra* note 69, ¶ 3.
72 *Id.* ¶ 2.
73 Nowak's Commentary, *supra* note 20, ¶ 17.
74 ICCPR, *supra* note 10, art. 4(1)
75 Nowak's Commentary, *supra* note 20, ¶ 26.
76 ICCPR, *supra* note 10, art. 40(2).
77 *Id.* art. 4(3); General Comment 29, *supra* note 69, ¶ 17.
78 General Comment 29, *supra* note 69, ¶ 17.
79 Lawless v. Ireland (no. 3) 332/57 Eur. Ct. H.R. 1961 ¶ 28.

the substantive[80] and the procedural[81] requirements set forth in Article 15(1) and (3) respectively. In the context of armed conflicts, the ECtHR considered the issue of derogation from Article 5 of the ECHR (right to liberty and security) in *Hassan v. United Kingdom*,[82] but there seem to be no specific instances thus far of States derogating from Article 8 obligations on the grounds of war or similar public emergency.

2 *Permissible Limitations*

States may be justified in limiting non-absolute rights on the basis of proscribed purposes, such as national security; public order, health, safety and morals; together with the protection of rights and freedoms of others.[83] Permissible limitations are subject to two conditions. First, the limitation must be proscribed by domestic law in that it has to have a clear legal basis.[84] This means that the law authorising the limitation of the given right must be publicly accessible, sufficiently precise and cannot confer unfettered discretion on those in charge of its execution.[85] Secondly, it must pursue a legitimate aim,[86] be reasonable, necessary and proportionate.[87] Thus, the restriction has to be necessary to achieve a legitimate objective, be rationally connected to attaining that purpose and be no more restrictive than required to do so.

As already observed, governments rarely choose to derogate from the obligations to protect the right to privacy, preferring instead to rely on permissible limitations clauses.[88] Recent decades have attested to a discernible trend in the practice of States restricting this right on the

80 ECHR, *supra* note 11, art. 15(1) stipulates three conditions, namely that: (1) there must be a public emergency threatening the life of the nation; (2) the measure taken in response to it must be strictly required by the exigencies of the situation; and (3) the measures taken must be in compliance with the Contracting Party's other obligations under international law.

81 *Id.* art. 15(3) requires that there is some formal or public act of derogation and that notice of derogation, measures adopted in consequence of it and of ending the derogation, is communicated to the Secretary-General of the Council of Europe.

82 Hassan v. United Kingdom (GC) 29750/09 Eur. Ct. H.R. 2014.

83 *See also* ICCPR, *supra* note 10, arts. 12(3), 18(3), 19(3), 21, 22; ECHR, *supra* note 11, arts. 9, 10, 11.

84 General Comment 16, *supra* note 19, ¶ 3.

85 *See also* General Comment 16, *supra* note 19, ¶ 8; U.N. Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); U.N. Human Rights Committee, Concluding Observations, Switzerland, ¶ 46, U.N. Doc. CCPR/C/CHE/CO/4 (July 27, 2017); Malone v. United Kingdom 8691/79 Eur.Ct.H.R. 1984; Zakharov v. Russia [GC] 47143/06, ¶ 228 Eur.Ct.H.R. 2015 (*Zakharov*); Szabó v. Hungary, ¶ 89, 48725/17 Eur. Ct. H.R. 2017 (*Szabó*).

86 *See* ICCPR, *supra* note 10, arts. 12(3), 18(3), 21 and 22(1); ECHR, *supra* note 11, art. 8(2); Martin Scheinin (Special Rapporteur), *Report on the Promotion and Protection of Human Rights while Countering Terrorism*, ¶¶ 17–18, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); *Zakharov*, ¶ 237.

87 *See also* U.N. Human Rights Committee, General Comment No. 27: Article 27 (Freedom of Movement), ¶¶ 14–15, U.N. Doc. CCPR/2/21/Rev1/Add9 (Nov. 2, 1999); S and Mapper v. United Kingdom, ¶ 118, 30562/04 Eur. Ct. H.R. (Dec. 4, 2008); *Zakharov*; *Szabó*; C-311/18 Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems, 2020, ¶ 185 ECLI:EU:C:2020:559.

88 U.N. Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, ¶ 15, U.N. Doc. A/HRC/27/37 (June 30, 2014) (A/HRC/27/37).

basis of new, or amended legislation that allows for far reaching State surveillance (such as bulk collection of communications' content and metadata) to facilitate fighting serious crime and cross-border terrorism. A case in point is the UK Investigatory Powers Act 2016;[89] the French Intelligence Act 2015;[90] and the Swedish Signals Intelligence Act 2016.[91] There are a number of reasons as to why the permissible limitations mechanism is preferable to derogations. First, States may find it difficult to show that the circumstances in question *de facto* threaten the life of the nation, as not every volatile situation necessarily reaches the threshold of an armed conflict within the meaning of common Article 2(1) to the Geneva Conventions. Second, permissible limitations are perceived as giving States sufficient leeway to achˇieve effective emergency responses, without having to give formal notification, or indeed provide reasons as to why they seek to do so and when the derogation would end. In addition, the limitations procedure seems to be more permissible in relation to the proportionality criteria which is common to the derogation and limitations powers. Under Article 4 of the ICCPR this must be justified by the exigencies of the situation, which is "a requirement that relates to the duration, geographical coverage and material scope of the state of emergency and any measures of derogation resorted to because of the emergency".[92] Furthermore, States must provide careful justification not only for their decision to proclaim a state of emergency, but also for any specific measure based on such a proclamation.[93] This can be contrasted with the interpretation of the proportionality criteria for the purposes of permissible limitations particularly in the context of the ECtHR case law addressing foreign surveillance of communications. The Strasbourg Court has long recognized that States face a difficult task of balancing national security and human rights, thus granting them a wide margin of discretion in regard to the implementation of security measures.[94] Finally, in a situation of armed conflict, States likely place little weight on their duty to respect and protect the right to privacy, as the requirements to adhere to other international law obligations, predominantly those set out by the rules of *jus in bello,* are probably considered as more pressing.

89 Investigatory Powers Act c. 25 2016.
90 French Intelligence Act (Law 2015-912) 2015.
91 Swedish Signals Intelligence Act 2016.
92 General Comment 29, *supra* note 69, ¶ 4.
93 *Id.* ¶ 5.
94 *See* Weber and Saravia v. Germany 54934/00 Eur. Ct. H.R. 2006; Liberty and Others v. United Kingdom 58234/00 Eur. Ct. H.R. 2008; Centrum För Rättvisa v. Sweden [GC] 3552/08 Eur. Ct. H.R. 2021; Big Brother Watch and Others v. United Kingdom 58170/13; 62322/14; 2460/15 Eur. Ct. H.R. 2021 (*Big Brother Watch*).

Equally, they might disregard the need for a formal derogation from privacy rights or even not countenance that they are bound by privacy and data protection obligations.

Bearing this in mind, the next section addresses the question of whether the right to privacy set out in international treaties applies in IAC and if so, how can they provide the normative foundations for States' drone surveillance operations.

III
THE RIGHT TO PRIVACY AND PROLONGED DRONE SURVEILLANCE IN ARMED CONFLICT — THE IHRL/IHL NEXUS

Privacy is not defined in international human rights treaties, but in essence it is "the presumption that individuals should have an area of autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals".[95] IHRL expressly recognizes privacy as a fundamental right and a rule of customary international law. A dense body of law and opinion has recently been developed at the UN and European levels pertaining to the right to privacy as a result of States' mass surveillance of digital communications, but the resultant courts' interpretation appears to be rather obfuscated. Thus, the UN human rights bodies and mandate holders acknowledge arbitrary interference and violation of this right, chiefly because bulk acquisition and retention of communications is seen as inherently disproportionate.[96] In contrast, the ECtHR has taken a more permissive stance, holding that such methods of intelligence gathering are an indispensable tool for States to safeguard national security, when that is undertaken in accordance with adequate safeguards and oversights mechanisms, which the Court's Grand Chamber set out in 2021 in *Big Brother Watch v. UK.*[97] Drone surveillance in situations of armed conflict is

95 A/HRC/25/59, *supra* note 6, ¶ 28.
96 *See* U N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/68/167 (Jan. 21, 2014); U.N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/69/166 (Feb. 10, 2015); U.N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/71/199 (Dec. 19, 2016).
97 *Big Brother Watch*, *supra* note 94.

equally if not more intrusive than bulk interception of digital communications in peacetime, as it directly encroaches on the privacy of home and family life, as well as data protection rights. With the increase in these activities and their almost certain spill over to situations which cannot be readily pigeonholed as an armed conflict in legal terms, it becomes imperative that militaries become mindful that privacy and data protection are legally binding rights also during hostilities in the absence of States' expressly derogating from them. The next section explores how this can be achieved.

A THE DUTY OF CONSTANT CARE AND DRONE SURVEILLANCE

The conceptual bridging of the IHRL/IHL gap in this context is the principle of constant care set out in Article 57 (1) of the AP I discussed above. As it likely applies to all military operations, it should arguably be extended to intelligence gathering by drones, placing a duty of care on military leaders to respect the privacy and data protection rights of civilian populations in their decision-making cycle. It is submitted that such a progressive interpretation of Article 57(1) could fill in the normative lacuna left by the IHL for at least five reasons.

First, it has been acknowledged that the constant care principle requires the commander to bear in mind the effects on the civilian population of what he or she is planning to do and take steps to reduce those effects as much as possible. This is recognized, *inter alia*, by the drafters of the *Tallinn Manual 2.0* in the context of States' cyber operations. To this end, the commentary to Rule 114 states that "in cyber operations, the duty of care requires commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon".[98] This supports a contention that Article 57(1) should capture all military activities associated with combat, including intelligence collection. Such an expansive interpretation of this provision is also garnering academic support. Thus, Asaf Lubin advocates that in the digital age, Article 57(1) should apply to "all informational operations necessary to support military activities", such as intelligence collection

98 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Michael N. Schmitt & Liis Vihul eds., Cambridge University Press 2017), Rule 114, ¶ 4 [hereinafter Tallinn Manual 2.0].

and broader data collection by any actor, including private contractors and civilian intelligence agencies, provided the necessary nexus exists between gathering, storing, processing and sharing and advancing combat.[99] Based on this reasoning, obtaining data from drone surveillance conducted with the view of combat throughout the entire spectrum of military operations should conceivably fall within the ambit of Article 57(1). This will place the necessity of amassing vast amounts of drone data within commanders' contemplation and entail a proportionality assessment. Thus, in implementing drone surveillance measures, militaries will be under an obligation to strike a balance between attaining the legitimate aim of target identification and safeguarding individuals' privacy rights, by imposing geographical and temporal limits on the surveillance and the amount of the collected data.

Second, the duty of care is constant which means it is of continuous nature and therefore does not have time limitations. The word "constant" according to the *Tallinn Manual 2.0* denotes that:

> the duty to take care to protect civilians and civilian objects is of a continuing nature throughout cyber operations; all those involved in the operation must discharge the duty. The law admits of no situation in which, or time when, individuals involved in the planning and execution process may ignore the effects of their operations on civilians or civilian objects. In the cyber context, this requires situational awareness at all times, not merely during the preparatory stage of an operation.[100]

It follows that duty of constant care likely arises at all stages of armed conflict — that is, before, during and after active hostilities.[101] Based on this reading, all information operations, including drone surveillance of civilians, irrespective of the stage of hostilities at which they are conducted, must be subject to this obligation.

Third, it is submitted that Article 57(1) should be interpreted in such a way as to recognize the type of harm inherent in prolonged surveillance, including continuous fear and trauma associated with a possible drone attack, interference with privacy and data protection implications. Admittedly the wording of Article 57(1) does not refer directly to harm,

99 Asaf Lubin, *The Duty of Constant Care and Data Protection in War*, *in* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD 10 (Laura A. Dickinson and Edward Berg eds., Oxford University Press, forthcoming, 2022).

100 TALLINN MANUAL 2.0, *supra* note 98, Rule 114, ¶ 5.

101 *See* Lubin, *supra* note 99, at 11.

stating merely that civilians and civilian objects must be spared. Article 57(2) then goes on to refer to "attacks" setting out a list of precautions that must be taken. This indicates that the drafters of AP I contemplated that the harm to civilian population is of a physical nature, such as death, personal injury and damage to civilian objects. However, as recognized by Lubin, in the information age there is a bundle of individual rights that have *digital* manifestation — that is, privacy, anonymity, access to information, online freedom of expression, digital autonomy and dignity, together with intellectual property.[102] As the right to privacy extends to the privacy of home and family life, individuals deserve protection against the harm caused by unrestrained drone surveillance by foreign militaries in particular because the strategic planning of militaries is increasingly swaying towards relying on technological tools such as machine learning and AI to enhance their military capabilities and decision making processes.[103] For this reason the duty of constant care should extend beyond physical harm and apply to protecting civilians from being subject to arbitrary interference with all aspects of their privacy, including the right to have a private sphere, that allows for autonomy and dignity.

Fourth, the duty of constant care should necessitate the adherence to the minimum data protection standards. This entails the protection of the data gathered in pursuance of intelligence operations from unrestricted collection, retention, processing and sharing. Strong support for such a progressive interpretation of Article 57(1) has been advanced in academic writing. For example, Lubin postulates that without any specific IHL rules in place, the duty of constant care as a data protection rule "stands as the only possible lighthouse that could guide militaries in discharging their duty".[104] In practical terms this would require commanders to take reasonable steps to reduce where feasible the negative effects on civilians of the information operations, through transplanting some of the fundamental principles of data protection such as that of fair, transparent and lawful processing onto the military theatre of operations.[105] To this end, fairness dictates that the collection and further processing of personal data must be carried out in such a way as not to interfere unreasonably

102 *Id.* at 14.

103 *See also* Stew Magnuson, *DoD Making Big Push to Catch up on Artificial Intelligence*, NATIONAL DEFENSE MAGAZINE (Mar. 16, 2017), https://www.nationaldefensemagazine.org/articles/2017/6/13/dod-making-big-push-to-catch-up-on-artificial-intelligence; Cade Metz, *As China Marchers Forward on A.I. the White House is Silent*, NEW YORK TIMES (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html.

104 Lubin, *supra* note 99, at 16.

105 *See also* Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, Jan. 28 1981, ETS 108 art. 5(a); General Data Protection Regulation, Apr. 27, 2016, OJ L 119, (GDPR) art. 5(1)(a).

with data subjects' privacy-related interests. This connotes proportionality in the balancing of interests of data subjects and data controllers and means that personal data must be "relevant" and "not excessive" in relation to the purpose for which it is processed.[106] Furthermore, the processing of personal data must be transparent for the data subjects, which means that data must not be processed surreptitiously, whilst data subjects must not be deceived as to the nature and purpose of the processing.[107] The principle of lawfulness requires that data processing may only be carried out pursuant to legal basis, which must specify the circumstances where such processing may be lawfully conducted.[108] As drone surveillance falls within military intelligence operations, the legality, fairness and transparency principles should apply, necessitating that the processing of data obtained through such methods complies with these basic requirements.

The prerequisite that surveillance be conducted on the basis of domestic law is also a fundamental principle of the right to privacy set out in, *inter alia,* Article 17 of the ICCPR and Article 8 of the ECHR. In interpreting this basic condition, the HRC stated that "interference authorised by States can only take place on the basis of the law, which itself must comply with the provisions, aims and objectives of the Covenant".[109] Moreover, in accordance with the principle of foreseeability, the law must be sufficiently clear to give an adequate indication of the circumstances and conditions empowering public authorities to resort to surveillance. In accordance with this stipulation, the ECtHR in the context of State interception of foreign communications developed minimum procedural standards in the 2006 case of *Weber v. Germany*[110] which laid down basic guarantees that a surveillance law must meet to be compliant with the ECHR. These safeguards have since been widened by the Grand Chamber of the ECtHR in *Big Brother Watch* v. *United Kingdom* and require the domestic legal frameworks to stipulate: (1) the grounds on which bulk interception may be authorised; (2) the circumstances in which an individual's communications may be intercepted; (3) the procedures to be followed for granting authorisation; (4) the procedures to be followed for selecting, examining and using intercepted material; (5) the precautions to be taken when communicating the material to other parties; (6) the limits on the duration of the interception, the storage of the intercept material and

106 Lee A. Bygrave, Data Privacy Law (Oxford University Press 2014), 148.
107 *Id.* at 147.
108 *See also* GDPR, art. 6(3).
109 General Comment 16, *supra* note 19, ¶ 3.
110 *See* Weber and Saravia v. Germany 54934/00 Eur. Ct. H.R. 2006, ¶ 95.

the circumstances in which such material must be erased or destroyed; (7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and (8) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[111] Drone surveillance—seen in the light of the principle of constant care—should be underpinned by the positive and continuous obligation of risk mitigation and harm prevention. This requires establishing minimum procedural safeguards which in turn entails adopting legislation delineating the circumstances in which such surveillance may be lawfully conducted. In practical terms, a starting point might be that the carrying out of drone surveillance is assessed on the basis of the aforementioned eight criteria and subject to *ex post* review of the reasons for the retention, sharing and other utilisation of drone data.

What can be concluded from the above analysis is a need for a two-pronged approach to prolonged drone surveillance in war zones. The first is to develop clear standards of when drones may be present in a given area setting out temporal and geographical limitations, together with the minimum procedural standards for conducting such surveillance. The second is to develop rules that address the processing, retention and sharing of the obtained data, imposing minimum data protection standards encompassing the concepts of legality, fairness and transparency. The rationale for this is the principle of constant care which must be interpreted to reflect the general aims of the Geneva Conventions and the Additional Protocols, namely to spare civilians from harm in times of war and to provide minimum protection to the victims of armed conflict by setting standards of humane treatment.

CONCLUSION

This chapter analyzed the issues concerning States' deployment of drones in wartime and the problems this creates outside of the usually discussed breaches of *jus ad bellum*, *jus in bello* and the right to life under international human rights law. Having demonstrated an individual and

111 *Big Brother Watch*, *supra* note 94, ¶ 361.

collective surge in the use of surveillance drones both in the context of international armed conflict and outside it, this chapter argued for a dualistic approach to these practices. The first necessitates developing procedural safeguards for States' deployment of surveillance drones. To assist in this, the set of guarantees stipulated by the ECtHR in the 2021 *Big Brother Watch* decision may be a useful benchmark to guide decisions made by militaries regarding the use of UAVs to obtain intelligence. This is due to the apparent similarities between these two methods of data acquisition, including their indiscriminate nature and the vast amounts of material obtained. The second is establishing data protection standards in line with the principles of legality, fairness, transparency and proportionality. Underpinning this contention is the principle of constant care which places a duty on military commanders to protect civilians throughout the entirety of military operations and means that those involved in the planning and execution process must not ignore the effects of their operations on civilians. In the digital age, this demands consideration be given to privacy and data protection rights of non-combatants in armed conflicts.