Journal of Conflict & Security Law © Oxford University Press 2018; All rights reserved.
For permissions, please e-mail: journals.permissions@oup.com
doi:10.1093/jcsl/kry008

Combat Drones: Hives, Swarms, and Autonomous Action?

Francis Grimal* and Jae Sundaram†

Abstract

From both *jus ad bellum* and *jus in bello* perspectives, the lawfulness of unmanned aerial vehicle/combat drone strikes have been examined extensively but not yet exhaustively. Recent advances in technology allow combat drones to operate as a swarm—similar to their vespidae counterparts. An overly simplistic conclusion would suggest that the current legal tapestry applicable to solo drone usage would 'automatically' apply to drones acting collectively or as a swarm. This article, however, posits a more controversial position that the technological uniqueness of individual drones acting as a swarm necessitates a more thorough deconstruction of the applicable legal framework. In other words, does the unique way in which a swarm operates lawfully comply with both *jus ad bellum* and *jus in bello* parameters? Crucial to this discussion, is to examine the extent to which a swarm is programmed both offensively and defensively—with a view to exploring the algorithm of an automated response from other drones within the swarm. Within this broader question, the article seeks to scrutinise two specific areas. First, to what extent is the drone swarm's architecture calibrated to comply with the cardinal self-defence parameters of necessity and proportionality should the swarm be attacked? And secondly, is the 'swarm' capable of being fully jus in bellow compliant in terms of distinction and proportionality and the duty to take precautions ('The General Principles'). Would, for example, the chain of command structure in a drone swarm encompass the concept of the 'reasonable military commander' when it comes to targeting? The purpose of this article is not to reopen, or indeed close the debate surrounding artificial intelligence and its ethical implications. Rather, it is to seek to open further discussion surrounding the applicability of 20th century legal thresholds to 21st century phenomena and beyond.

1. Introduction

A common misconception—albeit one which, does not permeate into scholarly literature, is that single drone usage is an entirely late 20th century phenomenon. This is simply not the case.[1] Similarly, while the 'swarming' of drones is

* University of Buckingham, UK. E-mail: francis.grimal@buckingham.ac.uk.
† University of Buckingham, UK. E-mail: jae.sundaram@buckingham.ac.uk. The authors would like to thank Professor James Green, Professor Marco Roscini, Professor Chris Waters, and Mr Ezequiel Heffes for their invaluable comments during the earlier stages of drafting this article.

1 See RP Barnidge, Jr, 'A Qualified Defense of American Drone Attacks in Northwest Pakistan Under International Humanitarian Law', (2012) 30 *Boston University*

undeniably a recent and unique phenomenon (hence the purpose of this article) 'swarming' as a battlefield strategy has been utilised previously.[2] What military structure or hierarchy would want to allow the swarm complete autonomy as to what to attack? With regards to the consensus model, the 'default' position is that military forces are not normally given freedom of manoeuvre—they are ordered/programmed what to do. This suggests that the Swarm operating under the consensus model would be no different. However, historical examples demonstrate that certain military operations (predating the swarming of unmanned aerial vehicles (UAVs)) have utilised swarming with this very approach in mind: individual elements within the swarm decide what target to engage. Burdick provides excellent coverage of the historical/strategic application noting that the German Stosstruppen (stormtroopers) and Japanese kamikazes employed swarming tactics 'to provide operational effects by destroying enemy forces and controlling geographic territory or sea space'. As Burdick elaborates, both examples only had the capacity to 'swarm' at local level unless receiving the green light from high command.[3] Burdick concludes (having surveyed the use of swarming in both the Battle of Britain and in Operation Desert Storm) that to conclude that strategic swarming has not been possible in the modern era is patently incorrect. Rather, he views (at least in relation to Desert Storm) 'that US airpower has not been deliberately structured for sustained swarming operations. Specific examples of tactical swarming may have occurred, yet they were usually brief, discrete, and/or unintended'.

The lawfulness and legality of single drone strikes from both *jus and bellum* and *jus in bello* angles continue to be afforded comprehensive scrutiny.[4] However, the present literature has yet to really consider the lawfulness or not as to the way in which a swarm operates and thoroughly deconstruct its compliance with the demands of both the *jus ad bellum* and the *jus in bello*. Recent tests and deployment of swarms albeit in a non-conflict context from the

International Law Journal 409–47, 413, noting that the first reported use of a 'drone' was in 1919, when a pilotless aircraft sunk a German battleship.

2 J Arquilla and D Ronfeldt, *Swarming and the Future of Conflict* (Rand Corporation, Santa Monica, 2000). The authors observe that swarming an adversary or, engaging an adversary from all directions simultaneously, either with fire or in force—is one of four types of doctrine that had been around for a long time. See also JE Burdick, 'Instantly Basis Locust Swarms: New Options for Future Air Operations' (Air University Press, Air University School of Advanced Air and Space Studies, 2016) 2. Burdick notes that the concept of swarming as a whole is nothing inherently new, citing the example of 'multidirectional hit-and-run tactics by irregular swarms of "shock troops" to exploit gaps and weaknesses in enemy lines of operation during World War I'.

3 Burdick's analyses the limitations of the Stosstruppen as follows: ' ... German Stosstruppen (storm troopers) were often dependent on exterior lines of communication for resupply, reinforcements, and artillery support'. Regarding the Kamikaze he notes that '... the effect of kamikaze forces was limited by aircraft range, their aircraft carrier's inventory of fuel and weapons, and the availability of qualified pilots'.

4 See fns 92 and 96 for a further clarification.

USA, Russian and Chinese Military make this topic open for a timely appraisal.[5]

To a greater degree, it can be said that there is less decision-making power vested in the human in a drone swarm operation than in comparison to a lone drone operation—as the drones in the swarm/formation are attributed with specific tasks which will be triggered off at individual points of the mission. However, on the other hand, there is an increased accountability to the actions of individual drones/robots used in a swarm. It is highly likely that in the very near future autonomous Global Position System (GPS) guided and drone swarms will become a mainstay in military affairs,[6] leading to various questions and claims arising from their actions.

One of the crucial remits of the work is to examine the legal consequences of actions taken in self-defence using an automated weapons system, and how this translates into a complex drone swarm scenario. The overarching goal of this article is to deconstruct the way in which a swarm may operate and ascertain its compliance (or not) within both the *jus ad bellum* and *jus in bello* frameworks.

Objectors could of course, argue that the legal issues raised here, are not unique to swarms of UAVs but rather relate to all manner of autonomous weapons system (AWS) and would go on to posit that if such differences exist, they derive from the degree of autonomous operation that the UAVs are capable of in terms of targeting, rather than the fact that multiple UAVs operate as a group. The authors, however, view that UAVs acting as a swarm is far more complex (depending on the architecture) than a single autonomous weapons system—it is at its simplest, a multi-autonomous set-up. While there already exists a substantial corpus of literature on autonomous weapon systems, the focus of this article is solely on the legal issues raised by swarms of UAVs. Again, one might concede that these relate to all manner of autonomous weapon systems, however, this article wishes to keep this focus on the specific nature of swarms. One might argue that UAVs are programmable devices rather than sentient entities. We are not seeking to reopen the perennial ethical debate surrounding drones and the nature of control by the drone operator which,

[5] KD Atherton, 'LOCUST Launcher Fires A Swarm of Navy Drones' (24 May 2016) <http://www.popsci.com/navys-locust-launcher-fires-swarm-drones> (accessed 20 September 2016). LOCUST stands for 'LOw-Cost Unmanned aerial vehicle Swarming Technology'; —'Russian 6th-Gen Drone Fighter Jets to Fly in Swarms, Enter Near Space' (12 July 2016) <https://www.rt.com/news/350736-russian-fighter-jets-drone-swarm/> (accessed 20 September 2016); D Hambling, 'If Drone Swarms are the Future, China May be Winning,' Popular Mechanics (23 December 2016) <http://www.popularmechanics.com/military/research/a24494/chinese-drones-swarms/> (accessed 31 May 2017).

[6] P Scharre, 'Robotics on the Battlefield Part II: The Coming Swarm' Center for New American Security (October 2014) 35, where the author notes that 'emerging robotic technologies will allow tomorrow's forces to fight as a swarm, with greater mass, coordination, intelligence and speed than today's networked forces'.

ultimately concludes that drones are not illegal weapons *per se* with regards to targeting because of human override and oversight.

To this end, Section 2 provides an overview of current technology and developments within the area of drone swarms. Section 3 considers the *jus ad bellum* question as to whether or not, and how a drone swarm is able to fully calibrate its action or response within the necessity and proportionality thresholds. More specifically, this area of analysis hones in on the scenario of an attack against a drone belonging to a swarm, and the immediate reaction in self-defence of the swarm itself. Section 4, meanwhile, will seek to frame the broader question of whether the unique behaviour of the swarm, particularly in terms of its responses, is fully IHL compliant. By way of overall conclusion, the authors position that the use of drone swarms is not inherently incompatible with *jus ad bellum* considerations. Equally, to categorically reject a swarms' compliance with IHL, would be patently incorrect. Rather, the article seeks to underscore that the variable of lawfulness firmly hinges not only on the swarm's architecture but also the chain of command.

2. Technological Overview and Current Developments

Combat drones as a single strike platform present the distinct strategic advantage of being 'unmanned'[7] and controlled remotely.[8] While a human element is undeniably present, the level of direct combat participation is far removed if one compares a UAV/Combat drone strike platform to that of an F-35. Unlike an F-35 pilot, the drone/UAV operator does not face the risk of being shot down. Some control, albeit remotely, is still in the hands of human operators. The undeniable strategic appeal of such a strike platform is a reduction in the number of possible human fatalities[9] that may arise from such 'air

[7] See NJ Cooke and RA Chadwick, 'Lessons Learned from Human-Robotic Interactions on the Ground and in the Air' in M Barnes and F Jentsch (eds), *Human-Robot Interaction in Future Military Operations* (Ashgate Publishing Ltd 2010) 355–72, where the authors state the view that the term 'unmanned' is a misnomer as UAVs are rife with human factors issues. Although the vehicle itself is uninhabited there are numerous personnel on the ground (command centre, etc) engaged in remote operation, sensing, communications, etc, and that the vehicles are not fully automated but remotely operated with various degrees of automation.

[8] GBA Ronconi, TJBatista and V Merola, 'The Utilization of Unmanned Aerial Vehicles (UAV) For Military Action in Foreign Airspace' *UFRGSMUN: UFRGS Model United Nations Journal* (2014) 137–82. Combat drones, referred to as UAVs and as remotely piloted vehicles, are pilotless aerial vehicles which can be guided either through remote control by a military squad in its home country, or that can navigate autonomously based on a pre-programmed software.

[9] ibid. See M Boot, 'The Paradox of Military Technology' *The New Atlantis* (2006) 13–31. Precision-Guided Munitions used in drone increases the accuracy of strikes to a point where it is possible to aim at a single human being and eventually hit it precisely, resulting in less fatalities.

strikes'.[10] When the numbers of the UAVs[11] are multiplied with each drone attributed a specific task and programmed to act in sync towards a particular strategic goal, a drone swam is created.[12] Here, individual drones are capable of navigating on their own while sharing information amongst themselves (dynamic information) and also to ground control station (GCS).[13] The GPS feeds information to the drones/swarm to ascertain their coordinates and plan and execute the flight.[14] Technologically speaking, drone swarms are used as force multipliers in the battlefield,[15] and are essentially networked drones.[16] Similar to multiple networked computers, drones are similarly networked to create a swarm, and to avoid any mid-air collisions.[17] Drone swarms are capable of 'collective motion' a behavioural trait observed in the animal kingdom. Bees, ants, birds, etc, are all capable of/exhibit collective motion whilst in flight mode, which is instinctual and well-coordinated.[18] This

[10] On this point, one could analogise, and refer to Turns' analysis on his piece on Cyber Warfare and direct participation in hostilities (DPH) in IHL. D Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) *Journal of Conflict & Security Law* 279–97. The authors are grateful to Professor JA Green who helpfully raised the idea (when commenting on an earlier draft) that within the context of international humanitarian law and direct participation in hostilities (in relation to remotely piloted or fully automated weapons) there cannot be a complete removal of human participation.

[11] For a definition and general discussion of UAVs, their development and applications, see K Nonami, F Kendoul, S Suzuki, W Wang and D Nakazawa, *Autonomous Flying Robots: Unmanned Aerial Vehicles and Micro Aerial Vehicles* (Springer, 2010). The authors also note that the main UAV applications are defence related and the investments are driven by future military scenarios.

[12] A Bürkle, F Segor and M Kollmann, 'Towards Autonomous Micro UAV Swarms' (2011) 61(1–4) *Journal of Intelligent and Robotic Systems* 339–53. See P Bhalla, 'Emerging Trends in Unmanned Aerial Systems' *Scholar Warrior* (Autumn, 2015) 86–94 <http://www.claws.in/images/journals_doc/1119543205_Emergingtrendsinunmannedaerialsystems.pdf> (accessed 20 September 2016).

[13] ibid. There is a dedicated channel between individual UAVs and the GCS to transmit status information from the UAVs and to receive commands from the GCS. There is also a dedicated data channel between individual UAVs and the GCS to send results of tasks. Also, a cooperative channel is opened between two UAVs, if one of them needs assistance to finish a task.

[14] Y Qu and Y Zhang, 'Cooperative Localization Against GPS Signal Loss in Multiple UAV Flights' (2011) 22(1) *Journal of Systems Engineering and Electronics* 103–12.

[15] Bürkle, Segor and Kollmann (n 12).

[16] Bhalla (n 12). The author identifies the swarms as a 'heterogeneous mix of machines with dissimilar tasks but contributing synergistically to the overall mission objectives'.

[17] K Kim, 'Integrating Coordinated Path Following Algorithms to Mitigate the Loss of Communication Among Multiple UAVs' (Master's thesis, Naval Postgraduate School, Monterey, California 2014); JD Foster, 'Swarming Unmanned Aerial Vehicles (UAVs): Extending Marine Aviation Ground Task Force Communications Using UAVs' (Master's thesis Naval Postgraduate School, Monterey, California 2014).

[18] This particular feature clearly demonstrates the emergence and the introduction of AI into the modern day battlespace in recent times.

particular feature of the drone swarms is highly desirable as it gives a tactical advantage, when it comes to manoeuvring in rugged terrains and amongst city scape.

Another quality that is found in a drone swarm is the division of labour, which is well demonstrated amongst bees, ants, etc.[19] For instance, in February 2016, Sistemprom, a Russian company unveiled a 'multicopter complex' which comprised a number of drones, with individual capabilities and specific tasks assigned to each drone in the formation.[20] They are decentralised when operating alone and when acting collectively, they perform a dynamic task with the objective of achieving a common goal.[21] Operating as a swarm, teams of less expensive drones can achieve more than a single drone/robot. This was demonstrated by the US Navy in May 2016 with the launch of its LOCUST Programme, where smaller, cheaper drones were used, with a single human controlling them from afar.[22] More recent innovations developed by Advanced Robotic Systems Engineering Laboratory (ARSENL)[23] have demonstrated that a single individual can control 50 drones at a given time, with the long goal to have the swarms determine how to act on their own, and to eventually have a drone swarm dogfight.[24] Currently, Arizona State University (ASU) is researching the possibility of mind-controlled drones/drone swarms, which would allow a single user to operate multiple drones through thought (brainwaves).[25] According to Panagiotis Artemiadis, director of the Human-Oriented Robotics and Control Lab at ASU, the future goal is to expand the research to include multiple swarms under the control of multiple people and sees the drones 'performing complex operations, such as search-and-rescue

[19] ibid.

[20] ___'Killer Drone Squad: Russia Unveils Anti-Armor Assault Multicoptor' (10 February 2016) <https://www.rt.com/news/332045-tank-destroyer-drone-complex/> (accessed 20 September 2016). The system comprises of four drones, *viz,* a robotic helicopter, sentinel multicopter, reconnaissance multicopter and an assault multicopter, with the drones capable of performing asks separately or jointly. JS Bellingham, M Tillerson, M Alighanbari, and JP How, 'Cooperative Path Planning for Multiple UAVs in Dynamic and Uncertain Environments' (Proceedings of the 41st IEEE Conference on Decision and Control, 2002) 2816–822; A Richards JS Bellingham, M Tillerson, and JP How, 'Coordination and Control of Multiple UAVs' in *AIAA Guidance, Navigation, and Control Conference, Monterey, California* (2002).

[21] ibid.

[22] Atherton (n 5).

[23] ARSENL, is part of the Naval Postgraduate School at Monterey, California. The team had previously launched 30 drones and controlled them simultaneously in July 2016. R Bishop, 'Record-Breaking Drone Swarm Sees 50 UAVs Controlled by a Single Person' (16 September 2016) <http://www.popularmechanics.com/flight/drones/news/a17371/record-breaking-drone-swarm/> (accessed 20 September 2016).

[24] ibid.

[25] R Alvarez, 'With This Interface One Person Can Control a Swarm of Drones With Their Mind' (18 July 2016) <http://thescienceexplorer.com/technology/interface-one-person-can-control-swarm-drones-their-mind> (accessed 20 September 2016).

missions'.[26] The Pentagon for its part has been experimenting with new prototypes, *viz*, microdrones that can be launched from the flare dispensers of moving F-16 s and F/A-18 fighter jets.[27] Although specifics of the capabilities of the mini drones remain classified, it is understood that they could be used to confuse enemy forces and carry out surveillance missions using equipment that costs much less than full-sized unmanned aircraft.[28]

In July 2016, Russia unveiled its sixth-generation drone fighter jets, which it claimed was largely consisted of unmanned aircrafts and drone swarms allowing a single-piloted aircraft command for up to 10 unmanned vehicles.[29] What is interesting about the Russian model is the command for the drone swarms comes from the pilot who is airborne and part of the formation, and as well as from the GCS, as opposed to only from the GCS. This is a departure from what has been witnessed in drone operations for over a decade. What we see here is a semi-autonomous robot, which is capable of performing certain tasks on its own, but still requiring human input in terms of decision-making, etc. The GCS plays an important role in supporting any mission for the drones and drone swarms, whilst also serving as the human interface to the drones and drone swarms in the air.[30]

The purpose of this present section is to consider the scientific and technological background that 'informs'/programmes a swarm's behaviour—namely swarm algorithm architecture; swarming in a network-centric warfare.[31] Such discussions will enable this article to more concretely address the *jus ad bellum* and *jus in bello* parameters and the way in which the swarm does or does not comply with those frameworks. The authors maintain as highlighted in the abstract, that the legal framework applicable to single-drone usage is not automatically transposed to that of a swarm—therefore, an understanding as to precisely how the swarm is configured and operates is paramount.

Therefore, the following issues need to be addressed from a technological perspective. First, is a swarm just one legal actor consisting of various parts,

[26] ibid.

[27] The experiment was run by the Strategic Capabilities Office, a secretive Pentagon organization launched in summer 2012 to counter growing strategic threats from China and Russia. See D Lamothe, 'Veil of Secrecy Lifted on Pentagon Office Planning Drone Swarms' *The Washington Post* (8 March 2016) <https://www.washingtonpost.com/news/checkpoint/wp/2016/03/08/inside-the-secretive-pentagon-office-planning-skyborg-fighters-and-drone-swarms/> (accessed 20 September 2016).

[28] ibid.

[29] See fn 5. It is claimed by the developers that the unmanned aircraft, flying at hypersonic speed would be able to interact and transit through space.

[30] KP Arnold, 'The UAV Ground Control Station: Types, Components, Safety, Redundancy, and Future Applications' (2016) 4(1) *International Journal of Unmanned Systems Engineering* 37–50.

[31] See eg J Lenahan, P Charles, R Reed, D Pacetti, and M Nash, 'Mapping Network Centric Operational Architectures to C2 and Software Architecture' Twelfth International Command and Control Research and Technology Symposium, 12th ICCRTS), 19–21 June 2007, Newport, (2007).

or does each part possess unique individual legal attributes? If it is the former, is it legally significant whether one deals with a drone swarm or an individual drone? If it is the latter, how does one determine which part possess separate attributes? And how would, in that case, a swarm be distinguished from other highly complex war machines, such as tanks or submarines that are all composed of an enormous number of sensors, parts, programs that all contribute to the versatility of the given machine?

In other words, to what extent could a drone swarm be compared to convoys of ships or formations of fighter planes—are the issues that a swarm raise in practice entirely novel? What exactly is the technical state of the art regarding a drone swarm? Which exact chain of command do the drone algorithms provide for? How is the degree of autonomy of a drone measured and how are swarms categorized by the various military powers around the world that use them? Given the volume of interrogatives posed, Section 2 will be subdivided into three distinct parts. Section A will address (from a technological perspective) whether a swarm is a single entity or comprises differing individual components—is the swarm simply to be treated as highly complex strike platform? Section B will then examine whether a swarm's behavioural pattern is simply analogous to that of a fighter squadron's tactical formation or whether there is something inherently unique about the way in which it operates—the view maintained by the current authors. Section C will inform the IHL discussion in Sections 3 and 4 of this article by considering the exact chain of command (C2) that the algorithms provide. Even if one were to concede that presently the swarm itself is analogous to that of a fighter squadron it is relatively uncontroversial to assert that this conclusion will soon be outdated.

A. Models of Swarm Architecture

Although swarming as a tactical/strategic military option has been in operation for centuries, it was not until recently that it had been explored as a serious option for application in modern warfare. Arquilla and Ronfeldt define swarming as 'a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions'.[32] This working definition of swarming presents a formula that could be adopted to warfare in all domains—land, water, air, space and possibly in cyberspace.[33]

Do drones within the swarm act individually or as a collective unit? This is very much dependent on how the Swarm is configured. Therefore, it is overly simplistic to conclude that it is either entirely individual or entirely collective. In

[32] Arquilla and Ronfeldt (n 2). The authors also note that in modern warfare swarming will only work if it is designed mainly around the deployment of myriad, small, dispersed, networked manoeuvre units—referred to as 'pods' organized in 'clusters'.

[33] The model propounded by Arquilla and Ronfeldt was primarily designed for 'netwar' and cyberwar.

order to capture and comprehend swarm architecture, it is necessary to explore some of the models that have been used in network-centric warfare over the decades. Just prior to this exploration, it is worth providing a brief overview along the following lines. Swarms invariably need a human commander at the mission level, giving overarching guidance, but delegated with a wide range of tasks to be carried out autonomously.[34] This capability could be enhanced through multivehicle control where a single individual tasks a group of vehicles that coordinates amongst themselves accomplish the task as a swarm.[35] For instance, an individual could task a swarm of missiles with a set of targets, but allow the missiles to coordinate among themselves to choose the target to strike.[36] Scharre observes that when the number of elements in a swarm increases, human control must shift increasingly to the swarm as a whole, rather than micromanaging individual elements, clearly implying that swarms are fully capable of operating autonomously to handle complex tasks.[37]

The 'Dekker Architecture' suggests several models including centralised NCW, hub request, hub swarm, joint, request based, mixed and swarming which, will be discussed shortly.[38] Even if at present it is the case of acting collectively, future technology would invariably lead towards greater independence from individual swarm members. Dekker, using the principles of swarming, developed a swarm architecture[39] broadly defined under four heads, based on a command and control structure (C2) for use in a NCW. It should be noted here that modern warfare is moving away from the platform-centric[40] approach of the last century towards a more network-centric approach with embedded nodal command and control structure.[41] Dekker's architecture broadly presents

[34] Scharre (n 6). The author also notes that in near term, this will entail a shift to mission-level-autonomy and multi-vehicle control, which would in turn require new command-and-control models to allow humans to employ large swarms effectively.

[35] ibid.

[36] ibid. The author notes that it is likely that a human could task a group of vehicles to maintain coverage over an area, for surveillance, communications relay, electronic warfare or to establish a defensive perimeter, and the vehicles might coordinate to determine how best to cover the area. The author also adds that the vehicles could exist across multiple domains, such as air, sea surface and undersea vehicles operating collectively with one person controlling the group

[37] ibid. The author points out that this area on exercising effective command-and-control over a swarm is still a nascent research.

[38] A Dekker, 'A Taxonomy of Network Centric Warfare Architectures' Defence Science and Technology Organisation, Canberra (Australia 2008). The Dekker architecture was developed to provide a taxonomy of possible NCW architecture, in order to illuminate the possible options for the Australian Defence Force.

[39] ibid.

[40] Viewed as the classic American way of war, platform centric warfare has historically been the way warfare was conducted since WWII by the USA. See AL Bailey, 'The Implications of Network Centric Warfare' (Army War College, Carlisle Barracks PA 2004).

[41] See AK Cebrowski, and JJ Garstka, 'Network-Centric Warfare: Its Origin and Future' (1998) 124(1) *US Naval Institute Proceedings*. The author notes that NCW derives its power from the strong networking of a well-informed but geographically dispersed

three NCW options, *viz*, a centralised model, a request-based model, and a swarming model. The centralised model has a single high-value central hub node, surrounded by a cluster of nodes of lower value—in the absence of the high-value hub the cluster of nodes of lower value may not be able to operate.[42] Under the request-based model presents the combination of fully value-symmetric and heterogeneous forces—a collection of pure specialists, all different, but all of equal value. Here, each node does only a few tasks, and does them extremely well—the result is a request-based architecture. The third model presented by Dekker is swarming, which is the combination of fully value-symmetric and homogenous forces of identical nodes. In this model, the nodes must share their sensor information, and self-synchronise so as to mass the effect of their weapons. Dekker further subdivides the swarming model as emergent swarming and situationally aware swarming.[43] By way of summary, it is important to note that Dekker's model/architecture does not explicitly refer to drone swarms. However, Dekker's model has then been adopted by other commentators such as Scharre and Burdick who then explicitly apply this to drone swarms.[44]

As Scharre notes, in more recent times concept for cooperative multi-vehicle control have been demonstrated in simulations and some real-world experiments,[45] and the operation of a drone swarm is technically feasible today.[46] Discussing the C2 models Scharre opines that to exercise effective command-and-control over a swarm is an area of nascent research, suggesting a possible C2 model ordered from more centralized to increasingly decentralized control.[47] Scharre's model encompasses four distinctively different NCWs, *viz*,

force. See also BC Logan, 'Technical Reference Model for Network-Centric Operations' (2003) 16(8) *Crosstalk* 22–25. The author notes that '… NCW is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness … .' See generally, DS Alberts, JJ Garstka and FP Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* Assistant Secretary of Defense (C3I/Command Control Research Program, Washington DC 2000).

42 Dekker compares the 'hub' to what Clausewitz called the 'centre of gravity …. on which everything depends'.

43 Dekker (n 38).

44 Burdick (n 2). The author uses the expression 'remotely piloted aircrafts' as opposed to drones.

45 Scharre (n 6).

46 It was reported in the early part of 2016 that the US Navy was preparing to fly a drone swarm through its Low-Cost Unmanned Aerial Vehicle Swarming Technology Program (LOCUST). See, D Hambling, 'US Navy Plans to Fly First Drone Swarm This Summer' *Defense Tech* (4 January 2016) <https://www.defensetech.org/2016/01/04/u-s-navy-plans-to-fly-first-drone-swarm-this-summer/> (15 March 2017).

47 Scharre (n 6). Scharre also takes the view that when the number of elements in a swarm increases, human control must shift increasingly to the swarm as a whole, rather than micromanaging individual elements.

> i) Centralized control model: *the swarm elements feed information back to a central planner which then tasks each element individually*.
> ii) Hierarchical control model: *the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher-level controllers, and so on.*
> iii) Coordination by consensus model: *the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.*
> iv) Emergent coordination model: *the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.*[48]

Complex swarm algorithms can be used for flight dynamics of individual as well as neighbouring aircraft, and essentially making the decisions for the swarm.[49] In 2014, a team of researchers led by Vijay Kumar from the University of Pennsylvania demonstrated their swarm-enabling algorithms.[50] Paul Burdick, in a study of the logistics requirements of remotely piloted aircrafts (RPAs), suggests that for a given situation, a fully autonomous RPA will fly according to the rule structures and algorithms (or parameters) programmed into its software.[51]

Importantly, Burdick notes that going by the Unmanned Systems Integrated Roadmap, human-supervised autonomous systems may be possible as early as 2018, and swarms of fully autonomous systems may pass research, development, test and evaluation (RDT&E) stages between 2020 and 2036.[52] Burdick also presents the argument that swarms may potentially have the ability to collectively change their radar signatures to mimic larger manned aircraft.[53] This could be possible as individual swarming aircraft/drones are small, and be able to fly in tight formations such that their radar signature appears similar to larger civilian or military aircraft.[54] Burdick also postulates the argument, that an RPA

[48] ibid.

[49] M Turpin, N Michael and V Kumar, 'Trajectory Design and Control for Aggressive Formation Flight with Quadrotors' (2012) 33(1–2) *Autonomous Robots* 143–56.

[50] See V Kumar, 'Vijay Kumar: Robots That Fly … and Cooperate', *TED.com* (February 2012) <https://www.ted.com/talks/vijay_kumar_robots_that_fly_and_cooperate> (accessed 21 March 2017). The algorithms enabled formations of quadrotor helicopters to accomplish multiple cooperative tasks, including advanced formation flight manoeuvres. German scientists A Bürkle, F Segor and M Kollman created sets of computer rules for collaborative micro RPA swarms, ground-based sensors, vehicles and ground control stations. See A Bürkle, F Segor and M Kollmann, 'Towards Autonomous Micro UAV Swarms', (2011) 61(1–4) *Journal of Intelligent and Robotic Systems* 339–53.

[51] Burdick (n 2). The author uses the expression 'remotely piloted aircrafts' as opposed to drones.

[52] DoD, US 'Unmanned Systems Integrated Roadmap FY2011–2036', (2013) 89 <https://fas.org/irp/program/collect/usroadmap2011.pdf> (accessed 23 October 2017).

[53] Burdick (n 2).

[54] ibid. Burdick also notes that the ability to change the shape of the swarm may also provide the ability to change radar signatures as desired by mission constraints.

swarm's kinetic payloads may provide sufficient force at much less cost than traditional aircraft.[55]

In summary, swarming is being extended to all domains of warfare, including to form a 'swarm of drones'. Here, each drone operating as a node is assigned with specific tasks, and drones in turn come together to act as a swarm through the use of rule structure, or algorithms.[56] The creation of drone swarms and their capabilities to be used in an NCW has now been established—both through theoretical expositions and field experiments. By way of conclusion therefore, Section A has underscored that a swarm can be seen as both individual and collective, but this very much depends on the model used to programme it. Thus, it is too simplistic to say that that swarm is either the sum of its parts or the whole.

B. The Human Presence

Is the swarm's behavioural pattern simply analogous to that of a fighter squadron's tactical formation and is there something inherently unique about the way in which it operates? This question, again, depends entirely on the rule structure/algorithm (the NCW/C2/CI4 model) that is programmed into the drone swarms which, is also subjectively dependant on the terrain and the task that has been assigned to the drone swarms. While it is impossible to avoid drawing parallels with a swarm's formation and that of any other battlefield formation (fighter squadron, fleet etc), the assertion repeated and maintained in Section B, is that the swarm is inherently unique but with the caveat this is contingent on the rule structure applied. To facilitate this discussion, it is necessary to briefly refer back to Scharre's model in Section A. As noted above, Scharre sets out four key models (all of which, are applicable to swarms):

> (i) Centralized control model: *the swarm elements feed information back to a central planner which then tasks each element individually*.
> (ii) Hierarchical control model: *the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher-level controllers, and so on.*

[55] ibid. The destructive power of lightweight bombs carried by swarming RPAs will likely increase over a period of time to deliver destructive power equivalent to the bombs loaded on today's manned combat aircraft, as ongoing research has already increased the destructive force of some explosives without increasing their weight or volume. See, J Gartner, 'Military Reloads with Nanotech' *MIT Technology Review* (21 January 2005) <https://www.technologyreview.com/s/403624/military-reloads-with-nanotech/> (accessed 22 March 2017).

[56] Algorithms that are programmed into individual nodes/drones can be seen as pre-made decisions, which process will repeat itself as long as the node is in operation, which is subject to its guidance system. See also Burdick (n 2).

(iii) Coordination by consensus model: *the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.*
(iv) Emergent coordination model: *the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.*

The question posed here is ultimately, where (i), (ii), (iii) or (iv) can be analogised to that of a fighter jet squadron. The premise maintained and presented is that a drone swarm is unique. The centralised control model (i) very much replicates that of a fighter jet squadron—while the pilots may communicate with one another, their overall mission statement is coordinated centrally by ground control. Therefore, the degree of autonomy to individual pilots is limited. Under the hierarchical control model, (ii) one could equally conclude that this also replicates the model used by a fighter squadron—there is a higher authority giving overall direction but the squadron leader maintains a degree of autonomy. The co-ordination by consensus model, (iii) is where one starts to notice an appreciable difference. Here, the drones would have the autonomy to take an autonomous decision between and amongst themselves, whereas the squadron (while the pilots may of course, communicate individually between each other) would still be ultimately in the hands of ground control in terms of target package etc. And finally, the emergent co-ordination model (iv) is inherently unique in terms of intuitive, since there is no need for communication with ground control. This is probably the clearest category to suggest that the drone swarm (under this architecture) is far more complex than that of a fighter squadron. Yes, one could posit that fighter pilots of a high degree of training may act in a similar way, but the level of intuition as to how the group operates falls far short as to that of a drone under this type of programming. Even if this view is rejected, the authors' maintain that it is simply a matter of time before it becomes so. Applying this back to the premise of B, depending which model is being used will, one could say that model (i) is indeed the equivalent of a fighter jet formation. However, if (ii), (iii) and (iv) are used then this suggests that the Swarm is indeed inherently unique.

C. Chain of Command

This section will primarily inform the discussion in Sections 3 and 4 of this article by considering the exact chain of command (C2) that the algorithms provide. Intrinsically linked to discussions concerning the uniqueness of a swarm presented in Section B is to understand the chain of command structure by which the swarm operates. The implications for the chain of command structure invariably surface when deconstructing the swarms' ability (or not) to comply with distinction, proportionality and the duty to take precautions ('The General Principles' of IHL) in Section 4. As noted in the abstract, would, for example, the chain of command structure in a drone swarm encompass the concept of the

'reasonable military commander' when it comes to targeting?[57] As with Sections A and B, the analysis will be grounded within the four models presented by Burdick and Scharre.

Recalling:

> i) Centralized control model: *the swarm elements feed information back to a central planner which then tasks each element individually*.
> ii) Hierarchical control model: *the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher-level controllers, and so on.*
> iii) Coordination by consensus model: *the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.*
> iv) Emergent coordination model: *the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.*

Under the centralized control model, (i) the chain of command is relatively straightforward and indeed comparable to that of a simple military command structure. According to Scharre and Brudick's centralized control model,[58] there would be effectively a 'lead' drone within the swarm dictating operations.[59] Within centralized control model, all nodes are identical.[60] As Lenahan notes, 'the choice of "leader" is therefore made on the basis of suitable position, current combat situation, or other transient factors'—an approach similar to that of special force teams whereby individuals can take operational command.[61] Lenahan further elaborates that in the event, the leader is unable to continue for any reason, the nodes agree on a replacement who, continues with the mission.[62]

The hierarchical control model (ii) meanwhile operates with a nodal system.[63] Each node in turn controls multiple subsets within the swarm that in turn could also be nodes.[64] Hierarchical Swarming as Dekker observes, replicates the more traditional military structure command and control C2 architecture.[65] Should one of the nodes become neutralized, the hierarchy is preserved via the promotion of other nodes—ensuring, that the commanding node retains the situational awareness it requires.[66] In terms of chain of command, 'the commanding node

[57] See RD Sloane, 'Puzzles of Proportion and the "Reasonable Military Commander": Reflections on the Law, Ethics, and Geopolitics of Proportionality', (2015) 6 *Harvard National Security Journal* 299–343. Also see the discussion in Section 4 of this article.
[58] Scharre (n 6); Brudick (n 2).
[59] ibid.
[60] Dekker (n 38); Lenahan and others (n 31).
[61] ibid.
[62] ibid.
[63] ibid.
[64] ibid.
[65] ibid.
[66] Dekker (n 38).

then produces a "big picture" plan (often called "intent"), this is passed down the hierarchy, and tactical detail is added by subordinate nodes'.[67] This means that at the start of each operation, the lead drone determines the battle plan and search pattern, including the number of servant drones required, and crucially, tasking each drone with their own specific operational remit.[68]

The co-ordination by consensus model (iii) [referred to some as distributed swarming] enables the swarm to operate without a discernible fixed chain of command—individual members within the swarm would vote as to their choice of action. In the more traditional sense, one could analogise that the commanding officer of a Special Forces operation has been neutralised and the remaining members of the squadron vote as to whether they proceed with the original mission brief. The chain of command model, therefore, is such that all decisions are achieved through consensus. Lenahan cautions that this model is confined to what he deems as simple 'problems'.[69] In other words, there would need to be a unitary decision and each node would have the same plan.[70] Furthermore, such a chain of command would require each node to have exactly the same situational awareness parameters—an issue which, as Lenahan notes, does not apply to most military operations.[71]

The fourth and final model, the emergent co-ordination model (iv) is more conceptually challenging. As with the coordination by consensus model, there is no visible chain of command. The Swarm acts 'organically' based on the emerging situation, shaped by external elements rather than a pre-determined course of action. One might suggest (this will be discussed further in Section 4) that this is a double-edged sword when it comes to IHL compliance.[72] On the one hand, one could controversially suggest that such intuitive action may enable the swarm to cease an attack within nanoseconds if, for example, the swarm ascertains that its original target, a building for example, no longer contains military personnel but is full of civilians.[73] However, on the minus side, intuitive action could result in a metaphorical 'rush of blood'—the swarm's intuition overrides its ability to make a more 'detached' assessment of its IHL obligations.[74] Clearly, one could be highly critical and reject the use of human metaphors (such as 'rush of blood') as they are inappropriate to describe actions undertaken by non-sentient beings. However, the authors maintain that while this may be the case, such language does 'capture' the idea of intuition.

[67] ibid; Lenahan and others (n 31).
[68] Lenahan and others (n 31).
[69] ibid.
[70] ibid.
[71] ibid.
[72] See discussion in Section 4(B).
[73] ibid.
[74] ibid.

3. Legal Framework from a *Jus ad Bellum* Perspective

A. Jus ad Bellum Framework

This section necessitates a brief overview of the *jus ad bellum* framework in order to ascertain the extent to which a defensive response by a swarm is fully *jus ad bellum* compliant. Article 2(4), or more precisely, the prohibition contained therein is absolute in terms of interdicting both threats and actual uses of force.[75] The views on the peremptory nature of the prohibition is varied—ranging from voicing caution against an overly liberal use of the peremptory status,[76] to arguing that the prohibition contained in Article 2(4) has peremptory status, and accordingly, cannot be derogated from.[77] For clarity and to avoid misinterpretation, it is important to stress that it is not Article 2(4) *per se* that has peremptory status, but rather, it is the prohibition of the use of force contained therein.[78] The UN Charter contains both a 'negative' prohibition, enshrined in Article 2(4) and a 'positive' duty, contained in Article 2(3), which requires Member States to settle their disputes resorting to peaceful methods. Article 2(7) of the UN Charter categorically states that the UN does not have the authority to intervene in a state's domestic affairs. The combined legal effect of Articles 2(3), 2(4) and 2(7) alongside the customary principle of non-intervention, provides a general obligation against states' interferingence in the sovereign affairs of other states.[79] The two permissible exceptions to the prohibition contained in Article 2(4) are self-defence and collective security. Since the remit of this article is centred on automated self-defence in the operation of drone swarms, the discussion will not venture into an examination of collective security. A further caveat is to note that a state's inherent right to

[75] This is area of the *jus ad bellum*, remains consistently subjected to careful scholarly attention. Francis Grimal and Jae Sundaram, Cyberwarfare and Autonomous Self-Defence, 4(2) Journal on the Use of Force and International Law (2017), 322 who note the following scholarly literature: O Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart 2010) 50–197; TM Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* (CUP 2002) 11–19; and N Schrijver, 'The Ban on the Use of Force in the UN Charter' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 466.

[76] JA Green, 'Questioning the Peremptory Status of the Prohibition of the Use of Force' (2010) 32 *Michigan Journal of International Law* 215.

[77] A Orakhelashvili, *Peremptory Norms in International Law* (OUP 2006).

[78] Green (n 76).

[79] Noting, that Treaties are interpreted according to the 1969 Vienna Convention on the Law of Treaties (VCLT). See also GI Tunkin, *Theory of International Law* (Wildy, Simmonds and Hill 2003) 141. See also the UN General Assembly Resolutions, *The Declaration on the Principles of International Law Concerning Friendly Relations and Cooperation Among States in accordance with the Charter of the United Nations* (A/RES/2625 (XXV) 24 October 1970) and *The Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*. (A/RES/42/22 November 1987).

invoke self-defence under customary international law is well documented, and therefore, this article will avoid opening 'old wounds'.

A state's inherent right of self-defence is contained both in pre-existing Charter law, in the form of customary international law, and Article 51 of the UN Charter.[80] In order for a state to invoke the right of self-defence, Article 51 requires that the state must have suffered an 'armed attack,' or at the very least be faced with a sufficiently serious and imminent threat of suffering an armed attack.[81] Unfortunately (and frustratingly), Article 51 remains silent as to what constitutes an 'armed attack', and the applicable threshold. The ICJ's judgment in the *Nicaragua* case[82] and scholarly commentary conclude that the threshold of an armed attack should be defined in the following terms: 'the most grave form of the use of force'—a qualitatively grave use of force—beyond a use of force simpliciter.[83] Ruys helpfully identifies that the ICJ's pronouncement in *Nicaragua* (in terms of requiring a certain 'scale and effect'—beyond a use of force simpliciter) has caused divisions within the literature whereby some bemoan the exclusion of 'mere frontier incidents' as satisfying the requisite threshold of Article 51.[84]

Having suffered an armed attack, the lawfulness of a state's response, is calibrated by the cardinal parameters of necessity and proportionality. Both necessity and proportionality are deep-rooted in customary international law, and were articulated in the correspondence between the then US Secretary of State Daniel Webster, and the British representative to the US, Lord Ashburton, with regards to and forming part of the *Caroline* incident dating back to 1837.[85] According to Daniel Webster, in order for a state to lawfully invoke self-defence it would need to:

[80] See Grimal and Sundaram (n 75), at 327, who note: JA Green and F Grimal, 'The Threat of Force as an Action in Self-Defense Under International Law' (2011) 44 *Vanderbilt Journal of Transnational Law* 285–329, 299.

[81] DW Greig, 'Self Defence and the Security Council: What Does Article 51 Require?' (1991) 40(2) *International and Comparative Law Quarterly* 366–402.nota bene: art 51 of the UN Charter remains silent as to imminence. For the more liberal view as to the possibility of self-defence against a sufficiently serious and imminent threat of suffering an armed attack, see Grimal and Sundaram (n 75), at 327, who note Terry D Gill, 'The Law of Armed Attack in the Context of the Nicaragua Case' (1989) 1 Hague Yearbook of International Law 30, 35.

[82] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (merits) [1986] ICJ Rep 14.

[83] Green and Grimal (n 80) 300; A Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Bruylant 2000) 57.

[84] T Ruys, *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge 2010) 140.

[85] Letter dated 27 July 1842, from Daniel Webster to Lord Ashburton (1841–42) XXX British and Foreign State Papers 193–4, extract taken from Webster's earlier letter to Henry S Fox dated 24 April 1841 (1840–1) XXIX British and Foreign State Papers 1137, 1137–8 (Caroline formula).

> [S]how a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation. It will be for it to show, also, that … [it] did nothing unreasonable or excessive; since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it.

The entwined principles of necessity and proportionality are derived from the Webster formulation.[86] De nos jours, necessity questions whether it was reasonable to use force as a last resort, and, if non-forcible measures were a reasonable alternative in the circumstances, that the state explored and exhausted those 'options'. It is also possible to pose the questions to establish a state's actions satisfy the requirement of necessity, as follows: (i) the state has exhausted all non-forcible measures[87] and (ii) it would be wholly unreasonable to expect the responding state to attempt a non-forcible response,[88] meaning that a 'forceful response' is a measure of last resort. Proportionality, meanwhile stipulates that the 'force employed must not be excessive with regard to the goal of abating or repelling the attack'.[89] Some commentators hold the view that a state's response need not actually mirror the initial attack, numerically speaking. For instance, if State A fires a dozen missiles at State B, then State B is not obligated under the concept of proportionality to respond in kind.[90]

One needs to bear in mind the distinction between the lawfulness of a defending state's action taken during an on-going armed attack—referred to as the

[86] See Green and Grimal (n 80) 299. See generally JA Green 'Docking the Caroline: Understanding the Relevance of the Formula in Contemporary Customary International Law Concerning Self-Defence' (2006) 14 *Cardozo Journal of International and Comparative Law* 429.

[87] Regarding this point on necessity, See Grimal and Sundaram (n 75), 327 who note: JA Green, 'The *Ratione Temporis* Elements of Self-Defence', (2015) 2(1) *Journal on the Use of Force in International Law* 100–01; G Schwarzenberger, 'The Fundamental Principles of International Law' (1955) 87 *Recueil Des Cours* 9, 97; Y Dinstein, *War, Aggression and Self-Defence* (CUP 2011) 187, 232; Green (n 76) 450–57; Ruys (n 84) 95–98; See M Williamson, *Terrorism, War and International Law: The Legality of the Use of Force against Afghanistan in 2001* (Ashgate 2009) 115; J Gardham, *Necessity, Proportionality, and the Use of Force by States* (CUP 2004) 6 and 11; and Green and Grimal (n 80) 300–02. See also *Case Concerning Oil Platforms* (*Islamic Republic of Iran v United States of America*) (merits) [2003] ICJ Rep 161, paras 63, 76 and 120.

[88] ibid. See *Case Concerning Oil Platforms*, ibid.

[89] Grimal and Sundaram (n 75) 328 who cite the following: See Constantinou (n 83) 159–61; GM Badr, 'The Exculpatory Effect of Self-Defense in State Responsibility' (1980) 10 *Georgia Journal of International and Comparative Law* 1; D Kretzmer, 'Killing of Suspected Terrorists: Extra Judicial Executions or Legitimate Means of Defence?' (2005) 16(2) *European Journal of International Law* 171–212.

[90] S Etezazian, 'The Nature of the Self-Defence Proportionality Requirement' (2016) 3(2) *Journal on the Use of Force and International Law* 260, 264–67; See *Legality of the Threat or Use of Nuclear Weapons* (advisory opinion) [1996] ICJ Rep 226, dissenting opinion of Judge Higgins, para 5. See also, generally, D Kretzmer, 'The Inherent Right to Self-Defence and Proportionality in *Jus ad Bellum*' (2013) 24(1) *European Journal of International Law* 235, 237; Green and Grimal (n 80) 301.

'cumulative effect' by Garwood-Gowers,[91] and instances where force continues to be employed after the cessation of the armed attack. In Green's view, in instances during an on-going armed attack, there must be a reasonable temporal proximity between the victim State's response and the armed attack itself.[92] Green adopts the position that the 'reasonableness' parameter is somewhat vague, and is certainly open to interpretation along the lines of 'a context-specific appraisal of the various factors that may delay a self-defence action: intelligence gathering, initial resort to negotiation, geographical disparity, and so on'.[93] This section has briefly sought to provide the basic topography and contours of the salient *jus ad bellum* considerations—in terms of the defensive aspects, enabling the following section to engage in a theoretical deconstruction of the *jus ad bellum* application. Typically, no discussion on self-defence is complete without the inclusion of the concept of imminence. Since the analysis presented in Section 3(B) is restricted to an actual 'armed attack' on the Swarm as opposed to the Swarm taking either anticipatory or pre-emptive action the article will not seek to reopen or apply this particular debate within the literature.[94]

B. Jus ad Bellum Application

Rather than revisit the thoroughly comprehensive corpus of literature surrounding lawfulness of drone strikes from a *jus ad bellum* perspective[95] the purpose of

[91] As noted by Grimal and Sundaram (n 75) 328. See generally, A Garwood-Gowers, 'Self-Defence Against Terrorism in the Post-9/11 World' (2004) 4 *Queensland University of Technology Law and Justice Journal* 1.

[92] As noted by Grimal and Sundaram (n 75). See JA Green 'The *Ratione Temporis* Elements of Self-Defence' (2015) 2(1) *Journal on the Use of Force and International Law* 97–118.

[93] ibid.

[94] By way of overview, state practice evidences not only that the attack must be imminent, but also reflects the ICJ's pronouncement that there is a further consideration—that the imminent attack must attain a certain threshold in terms of gravity (ie, there needs to be an imminent 'armed attack'). See NA Shah, 'Self-Defence, Anticipatory Self-Defence and Pre-Emption: International Law's Response to Terrorism' (2007) 12(1) *Journal of Conflict and Security Law* 95, 101–4, 111–19 (describing the gravity and immediacy of the threat required to justify self-defence under international law).

[95] On this point, see eg C Henderson, 'Introducing Perspectives on the Joint Committee's Drones Report', (2016) 3(2) *Journal on the Use of Force and International Law* 194–97; C Gray, 'Targeted Killing Outside Armed Conflict: A New Departure for the UK', (2016) 3(2) *Journal on the Use of Force and International Law* 198–204; ME O'Connell, 'The Law on the Lethal Force Begins with the Right to Life', (2016) 3(2) *Journal on the Use of Force and International Law* 204–09; ND White, 'The Joint Committee, Drone Strikes and Self-Defence: Caught in No Man's Land?' (2016) 3(2) *Journal on the Use of Force and International Law* 210–16; K Bannelier-Christakis, 'The Joint Committee's, Drones Report: Far-Reaching Conclusions on Self-Defence Based on a Dubious Reading of Resolution 2249' (2016) 3(2) *Journal on the Use of Force and International Law*

this section is to pose and deconstruct one key, fundamental question. Does the automated response by a swarm satisfy the necessity and proportionality requirements needed for the lawful invocation of self-defence? The scenario envisaged here is assuming one member of the swarm is attacked/neutralised, how would the response of the swarm itself need to manifest itself in order to comply with a state's inherent right of self-defence? In order to more forensically address this broader, overarching question, the authors propose to use the four models of network drone swarming set out in Section 2 as a framework for analysis. Depending on the specific architecture of the swarm the lawfulness of its actions may be affected.

Before delving into specifics, the following observations may be presented by way of overview. If one single drone within the swarm is attacked, would that satisfy the grave use of force threshold required by Article 51 to constitute an 'armed attack'[96] thus enabling the swarm to invoke an automated response in self-defence? The first observation to underscore is that by 'automated', the authors use this to describe an action whereby the weapons system itself responds automatically—the system assesses that it has been attacked albeit within micro seconds and responds immediately to the attack. A response in self-defence by its very nature is not inherently autonomous—a state or more specifically a weapons system can choose not to 'reply' to the initial armed attack unless programmed otherwise. One could similarly analogise as to whether a state would view the downing of a sole military jet within a formation as constituting an armed attack. However, providing the attack does meet the armed attack threshold, clearly the response would have to comply with necessity and proportionality. This invites the question as to the extent to which the UAVs programmed to make the call that all non-forceful measure have been exhausted, and whether it would be wholly unreasonable to expect a non-forceful response—bearing in mind that the swarm would undertake such calculations. Proportionality wise, the response would have to be in line with the defensive necessity of abating or repelling a further attack.[97] In this sense, if the swarm's response is simply to 'take out' the attacker, eg an anti-drone system (akin to a Missile Defence Shield)[98]—one could argue that this response would probably fall within the applicable framework and the action be rendered lawful.

217–26; S Breau, 'Reflections on the Treatment of the Decision-Making Process in Section 4 of the Joint Committee's Drone Strikes Report' (2016) 3(2) *Journal on the Use of Force and International Law* 227–33. See also, A Chehtman, 'The ad bellum Challenge of Drones: Recalibrating Permissible Use of Force', (2017) 28(1) *European Journal of International Law* 173–97.

96 See *Nicaragua* case (n 82).

97 Etezazian (n 90); see *Nuclear Weapons* (advisory opinion) n 90. See also, generally, Kretzmer (n 90); Green and Grimal (n 80) 301.

98 For further discussion on this, see eg F Grimal, 'Missile Defence Shields: Automated and Anticipatory Self-defence?' (2014) 19(2) *Journal of Conflict and Security Law* 317–39.

In effect, there are two variables at play: the architecture itself (ie the model used) and the algorithms used in the programming of individual drones. One could say that depending on which model is used, the temporal considerations are also altered; albeit within nanoseconds. The consensus model for example, would require a longer timeframe for the swarm to vote on action as opposed to a more immediate response. In terms of the temporal requirements of self-defence, this poses no real problem—the response is still within a very constrained timeframe—it is proximate, but there may be differing responses between the different models in terms of reaction times. The authors propose that depending on the model/architecture utilised may affect the degree of lawfulness in terms of the extent to which the swarm can satisfy the necessity and proportionality requirements but that this is underpinned by the extent of the programming itself. Models (i), (ii) and (iii) are probably capable of complying with the self-defence parameters whereas the unpredictability of model (iv) does invite the question as to whether that swarm architecture is compliant.

> (i) Centralized control model: *the swarm elements feed information back to a central planner which then tasks each element individually*.

Under the centralized control model, one could posit that the mechanism for assessing and calibrating the response in terms of necessity and proportionality is greatly assisted by the fact the decision is taken back at 'command and control'. While the swarm itself may not benefit strategically—it may take longer for the swarm to be able to defend itself in terms of taking self-defence action but from a legal perspective, it is easier to prove that the swarm is satisfying the necessity element of the concept of last resort.

> ii) Hierarchical control model: *the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher-level controllers, and so on.*

Similar to the centralized control model, one could submit that the same conclusions are equally applicable within this architectural set-up. The idea of a hierarchical decision suggests that there is again, greater scope for ensuing compliance albeit theoretically. The swarm is subject to an oversight process in terms of whether a decision for it to respond is taken. However, one could of course, quickly counter that this again depends entirely on the programming—a 'poorly' programmed higher level control may not necessarily reach the correct 'legal' decision.

> iii) Coordination by consensus model: *the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.*

Depending on the model, could affect the way in which the 'decision' to respond is taken. Under the consensus model, all members within the swarm would presumably have to vote as a unit as to whether they collectively view that the necessity element has been satisfied, and whether the proposed course of action would be proportionate to the defensive necessity of abating or repelling an attack.

> iv) Emergent coordination model: *the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.*

This is possibly the most problematic model in terms of compliance. Given the reaction is 'intuitive'/organic, this begs the question as to whether that architecture would compute the legal requirements in the same way—subject of course to programming. Perhaps, here, there is too great a degree of autonomy to the swarm as to whether it may comply with necessity and proportionality. A further 'footnote' to this section is to underscore whether the rules of engagement would change in terms of a swarm shooting down a single drone incursion into its territory. Would the swarm escort the single drone out of its airspace?

4. IHL Compliance?

A. Jus in Bello Considerations

For the purposes of this article, and given the nature of the enquiry into swarm behaviour (the swarm as a method of warfare), analysis of *jus in bello* considerations will be limited to that of targeting, since that is the primary area of interest in terms of calibrating 'swarm compliance'.[99] At this juncture, it is perhaps necessary to provide a brief overview regarding the overall applicable framework and the context within which IHL operates. As a basic precept of IHL, the starting point is to underscore that IHL will only be applicable if the Swarm is acting in the context of an armed conflict.[100] If such action falls outside the context of an international armed conflict (IAC) or indeed a non-international armed conflict (NIAC),[101] then the applicable law is the less lenient and

[99] For a very useful overview regarding regulation of combat drones, see C Heyns and others, 'The International Law Framework Regulating the Use of Armed Drones' (2016) 64(4) *International and Comparative Law Quarterly* 791–827.

[100] Generally, art 2 of the Geneva Conventions where their scope of application is defined, one could also include the definition for IACs given in art 2(2) and for NIACs in *Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction in Prosecutor v Tadic*, 1995, para 70. See generally R Kolb, *Advanced Introduction to International Humanitarian Law* (Edward Elgar Publishing 2014).

[101] nota bene: it is important to state that this is not the only scenario outside of an international armed conflict. For example, what if such actions take place during peacetime? Would it be possibly for the swarm to use force without technically triggering International Humanitarian Law? The authors concede that while this

more restrictive (when it comes to having recourse to lethal force) corpus found within international human rights law.[102] Under the European Convention on Human Rights, lethal force is only permissible in three specific instances: first, if it is absolutely necessary to prevent or protect loss of human life in the face of an unlawful use of force.[103] Secondly, lethal force may be permissible if it is used to execute an arrest.[104] And thirdly, lethal force may be authorised if it is to quell a riot or insurrection.[105] As Roscini notes, the transition from European Convention on Human Rights (ECHR) provisions in peace time to IHL in the context of an armed conflict tracks a shift in perspective—lethal force is no longer protective but is now justified on the grounds of achieving a military advantage.[106]

Having briefly noted the applicable framework, the attention will now turn to briefly unpicking the parameters surrounding targeting. Targeting, simply

possibility is theoretically conceivable, the likelihood of swarm deployment during peacetime is more remote. As Lubell notes, following *Tadic*, 'under customary international law the IHL rules on international and non-international armed conflicts are in essence much the same and according to the International Committee of the Red Cross (ICRC) study the majority of IHL rules (though not all) apply to both types of conflict'. N Lubell, 'Challenges in Applying Human Rights Law to Armed Conflict' (2005) 187(860) *IRRC* 747.

[102] See ICRC Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' *Power of Humanity, 32nd International Conference of the Red Cross and Red Crescent* (8–10 July 2015) <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> (accessed 9 August 2016). See 34, where the important differences between the conduct of hostilities and law-enforcement paradigms are highlighted. Principles of necessity, proportionality and precautions exist in both, but have distinct meanings and operate differently. While the conduct of hostilities paradigm allows lethal force to be directed against lawful targets as a first resort, the use of lethal force in law-enforcement operations may be employed only as a last resort, subject to strict or absolute necessity. This is the view seemingly posited by M Roscini. Roscini believes that a fully autonomous UAS/UCAS could meet the principles of distinctio, particularly in areas with little, or no civilians. See M Roscini, see Professor C Coke and Dr M Roscini, 'Transcript – Drones: The Future of War?' (*Chatham House*, 8 April 2013) , p. 10. <https://www.chathamhouse.org/sites/files/chathamhouse/public/Meetings/Meeting%20Transcripts/080413Drones.pdf> (31 May 2017). However, one could also suggest that if it happens in the context of a NIAC then the applicable law is the IHL on NIACs (alongside International Human Rights Law (IHRL)).

[103] ibid. Given that Roscini enshrines his arguments within the context of the ECHR, the authors of this article have proceeded on similar grounds. However, it should be noted for completeness, that the ICCPR would be equally if not more so applicable than a more regional treaty such as the ECHR.

[104] ibid.

[105] ibid.

[106] This implicitly recognizes the *lex specialis* maxim. See *Nuclear Weapons* (advisory opinion) (n 90) para 25; M Sassòli and LM Olson, 'The Relationship Between International Humanitarian and Human Rights Law Where it Matters: Admissible Killing and Internment of Fighters in Non-International Armed Conflicts', (2008) 90 (871) *International Review of the Red Cross* 599–627.

put, is what is lawful and what is not in the context of an attack.[107] Like its self-defence counterpart within the *jus ad bellum*, two key parameters operate within the *jus in bello* in order to ensure that action is IHL compliant: distinction and proportionality.[108] The first is distinction, which, categorically and emphatically prohibits the direct attack on both civilians and civilian objects.[109] To do so constitutes a war crime.[110] The second is proportionality.

While proportionality is codified within Protocol to 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 (API) 51(5)(b) the actual terminology passes without direct mention within the actual text.[111] In a similar vein to its direct *jus ad bellum* namesake, it is fully enshrined both within customary international law and treaty law.[112] Proportionality balances two critical elements/values: damage (incidental) and military advantage

[107] Roscini (n 99). G Corn, JA Schoettler Jr, 'Targeting and Civilian Risk Mitigation: The Essential Role of Precautionary Measures', (2015) 223(4) *Military Law Review* 785, 787; MN Schmitt and EW Widmar, '"On Target": Precision and Balance in the Contemporary Law of Targeting', (2014) 7 *Journal of National Security Law and Policy* 379.

[108] Noting, of course, that these operate alongside a general duty and obligation to take precautions to prevent incidental loss of life. See Y Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (CUP 2010).

[109] ibid. See ICRC Customary base referring to the first rule. J-M Henckaerts and L Doswald-Beck (eds), *Customary International Humanitarian Law Vol 1* (CUP 2009) 3–8. See also art 48 AP I and Additional Protocol I, arts 51(2), 52(1); Additional Protocol II, art 13(2) (The civilian population); CHIL, Rules 1 and 7 Additional Protocol I, art 51(4); CIHL, (ICRC) Rule 11. Additional Protocol I, art 51(5)(b); CIHL, (ICRC) Rule 14. Additional Protocol I, art 57; CIHL, (ICRC) Rule 15–24.

[110] K Dörmann, *Elements of War Crimes under the Rome Statute of the International Criminal Court: Sources and Commentary*, (CUP 2003) 130 and 233. See the Judgment in *The Prosecutor v Stanislav Galic* – Case No IT-98-29-T (5 December 2010) Trial Chamber I <http://www.icty.org/x/file/Legal%20Library/jud_supplement/supp46-e/galic.htm> (11 October 2016). However, not all attacks on civilians necessarily a war crime. See Second Provision Rome Statute noting the word 'intentionally'—there must be intention present:
Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.

[111] C Pilloud and others, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers 1987) 625–26, where it is stated that this provision 'should therefore lead those responsible for such attacks to take all necessary precautions before making their decision, even in the difficult constraints of battle conditions'.

[112] Proportionality is also fully operable in the context of a NIAC. See ICRC Customary Rule 14. See J-M Henckaerts and others, 'Customary International Humanitarian Law: Other Persons Afforded Specific Protection' (Rules 134–38) 46–50.

whereby one must not be excessive to the other.[113] If the incidental loss of life is excessive to the supposed military gain, it could be considered as an indiscriminate attack.[114] This (incidental damage) becomes particularly apparent when a target has dual use such as a power station.[115] Military advantage must be concrete and direct following the requirements set out in Article 57(2)(a)(ii) found within API. Schmitt and Thurner in their seminal work, explore whether autonomous weapon systems are capable of performing proportionality calculations noting, that such calculations would require consideration by the AWS of expected collateral damage and anticipated military advantage.[116] As Schmitt and Thurner acknowledge, this is a certainly a theoretical possibility, were the swarm 'be pre-programmed with unacceptable collateral damage thresholds for particular target sets or situations' along the lines of collateral damage methodology.[117]

More problematic however, is actually when and how proportionality applies as highlighted in the Final Report of the ICTY Committee on the North Atlantic Treaty Organization (NATO) bombings.[118] Broadly speaking, there must be an attack as required by Article 49 API within which, there is an act of violence, non-violent military harm is not enough resulting in loss of life to persons or property—there is some sort of kinetic or physical damage.[119] Alongside distinction and proportionality operates the third element: (forming the 'Principles' of IHL) the duty to take precautions when conducting an attack.[120] The other

[113] Rule 14 explicitly states that, 'Launching an attack 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, is prohibited'. While ICRC customary rules provide an invaluable interpretative source of customary IHL, they are of course non-binding: International Committee of the Red Cross, *Customary International Humanitarian Law Vol 1: Rules,* (CUP 2009) - (hereinafter ICRC Rules).

[114] art 51(5)(b): Among others, the following types of attacks are to be considered as indiscriminate: (a)... (b) an attack 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.

[115] M Sassòli, 'Legitimate Targets of Attacks under International Humanitarian Law' (2003) 7 *HPCR Policy Brief*.

[116] See M Schimitt and J Thurner '"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict', (2013) 4 *Harvard National Security Journal* 231–81. Schimitt and Thurner note that '(CDEM) is a procedure whereby an attacking force considers such factors as the precision of a weapon, its blast effect, attack tactics, the probability of civilian presence in structures near the target, and the composition of structures to estimate the number of civilian casualties likely to be caused during an attack'.

[117] ibid. The authors although do not refer to a 'drone swarm' but to an autonomous weapons system.

[118] Roscini (n 102).

[119] ibid.

[120] JJ-F Quéguiner, 'Precautions Under the Law Governing the Conduct of Hostilities' (2006) 88(864) *International Review of the Red Cross* 793–821.

element to note, is the requirement under Article 49 API in terms of an 'attack'—this can either be offensive or defensive, and it is generally uncontroversial that non-violent military harm is not enough to turn an act of hostility into an attack for the purposes of A49 API.[121]

Finally, and perhaps most interesting of all is the concept of the 'reasonable military commander'.[122] Conceived ostensibly, by the ICTY Committee on the NATO bombings, the idea of the reasonable military commander attempts to find a *juste milieu* between the more hawkish nature of IHL and the pacific aspect of IHRL from the perspective of command responsibility.[123] The creation of the reasonable military commander attempts to guide the precarious balancing act between anticipating the military advantage against the expected incidental damage.[124] Even if undertaken due diligently, one might say that this perhaps somewhat uncharitably involves an element of subjective/'guess work'—the reasonable military commander, therefore, seeks to provide a more objective approach.[125] Clearly, if the calculated effects of the attack are entirely unclear and unforeseeable the attack is like to be indiscriminate and, therefore, prohibited under IHL.[126]

B. Jus in Bello Application

Given the breadth and depth of existing analysis surrounding a sole combat drone's compliance or, indeed, possible non-compliance with IHL, the article will not seek to reopen pre-existing debate.[127] Rather, the discussion will be specifically limited to how drones attacking as a swarm would fall within the IHL framework. This present section will adopt the same four models considered in Section 3(B) and analyse whether the differing architectures, affects the swarm's potential to comply with the key principles of IHL alongside the concept of the reasonable military commander. Clearly, the same caveats raised in terms of *jus ad bellum* considerations are also applicable: much will depend on the nature of the task, the architecture used and the way in which the algorithms have been preset. This section will confine itself to swarm compliance of IHL solely to the aspect of targeting.

[121] M Roscini, *Cyber Operations and Use of Force in International Law* (Oxford 2014) 178.
[122] Sloane (n 57); MN Schmitt, L Arimatsu and T McCormack (eds), *Yearbook of International Humanitarian Law-2010* (Springer 2011) 193; Roscini (n 121) 228.
[123] ibid.
[124] ibid.
[125] ibid.
[126] ibid.
[127] See Heyns and others (n 99) for a very comprehensive discussion on single combat drone / UAV compliance with IHL.

i) Centralized control model: *the swarm elements feed information back to a central planner which then tasks each element individually*.

In terms of distinction, the centralized control model offers less variance than the emergent co-ordination model, and one could therefore, conclude that there would be greater oversight in terms of ensuring that the 'targeteer', in this case the central planner, is IHL compliant. The swarm is relaying information back centrally and so, in theory at least, the element of autonomous action is limited to a certain degree. Proportionality wise, one could also suggest that providing the central planner is indeed a 'reasonable military commander', the swarm's actions have a degree of oversight. Clearly, and as with all models, if one were to say that the swarm is inherently incapable of satisfying any of the IHL parameters, the swarm's actions would be in violation of IHL—something addressed further in the conclusion to this section.

ii) Hierarchical control model: *the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher-level controllers, and so on.*

While there is an overall hierarchical set-up, there is a greater degree of autonomy to the swarm itself—the swarm is controlled by squad-level agents. The hierarchical control model presents a slightly more problematic picture. Could the squad-level agents successfully balance the incidental damage on civilians and civilian objects versus the concrete and direct military advantage? Would the swarm 'appreciate' the complexities of targeting a dual use power station where it would theoretically need to account not only for the loss of civilian function but also the consequences—recalling of course, that the military advantage must be concrete and direct. Equally, and within the concept of concrete and direct military advantage, one can refer of course to the ICRC's definition that this encompasses the concept of ground gained and the weakening/annihilation of the enemy's military force.[128] In a similar vein to the threshold of a cyberattack (in terms of a concrete and direct military advantage), one could draw a similar conclusion to that of Roscini—if that calculation encompasses protection of the attacking forces then the incidental damage has to also be proportionately higher. Here, and as with a cyberattack, one could view that the lack of human involvement (the swarms are of course the elements at risk), the incidental damage that the swarm may cause also has to be held to a much higher account. As Roscini himself recognises in the context of a cyberattack, this becomes a very subjective balancing act.

[128] See Roscini (n 121) 224, who notes that there is limited state practice (Canada, Australia, New Zealand and Israel to support the view that when calculating concrete and direct military advantage, the protection of the attacking forces should also be a consideration.

In sum, the precautions adopted by a belligerent state under API are as follows: using a mode or method of attack to avoid and minimise the incidental loss of civilian life and damage to civilian objects. One could suggest that the hierarchical control model—due to the 'agency' of the squad-level operators have potential difficulty here. Would the hierarchical model allow for 'feasible precautions'[129] (this includes the protection of the attacking forces who are under no obligation to sacrifice themselves)—the swarm itself may wish to self-preserve. And finally, the duty to take precautions means that the mode of warfare utilised may well minimise the risk to the attacking forces (in which case the swarm) even if this decreases them military advantage, providing of course that this has no bearing on the expected incidental damage on civilians or civilian objects. [130]

iii) Coordination by consensus model: *the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.*

Many of the same concerns raised with regards to the hierarchical model present themselves to the co-ordination by consensus model so rather than revisit each one individually, it perhaps makes more sense to raise points of departure. The key concern with the co-ordination by consensus model magnifies the problems in complying with all the key IHL aspects. Providing of course the swarm is 'correctly' programmed, this is not an issue but one could easily flag up an instance whereby the swarm is voting as to whether it should attack, for example, a dual use infrastructure. One could be equally measured and say that this is not too dissimilar to a regular infantry unit deciding on whether they launch an artillery attack. However, the overwhelming concern is that lack of the presence of a 'reasonable military commander' to evaluate the proportionality elements of the proposed attack.

iv) Emergent coordination model: *the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.*

Finally, the emergent co-ordination model suggests an increasingly high level of autonomy (perhaps complete autonomy effectively) to the swarm. The overriding concern here is that the Swarm is left to its own devices. In of itself one could counter argue and say that providing the programming of all the algorithms correctly equates for distinction, proportionality, duty to take precautions etc, the swarm may still be IHL compliant. However, the reality is that such autonomy does, as with all autonomous systems raise the question as to

[129] ibid. 219.
[130] Roscini (n 121).

whether the swarm could distinguish its targets correctly, balance the loss of civilian life against the direct and concrete military advantage and take the necessary precautions without entirely without the presence of a reasonable military commander. Unless of course, the concept of the reasonable military commander is built into the software. In summary, the overarching suggestion is that the greater level of autonomy to the swarm under (ii) – (iv) may pose problems in terms of IHL compliance. More generally, in terms of autonomous weapon systems as a whole, and following the Roscini line of thinking (who dismisses the notion that autonomous systems are incapable of ever being compatible with IHL), the authors of this article, take a similarly measured view.[131] It is less about whether the swarm does or does not violate IHL and more about how the operations fit within the existing framework. Clearly, if the swarm is incapable of fulfilling the distinction requirement, its use is inherently unlawful.[132]

A basic tenet of IHL is that the commander must operate in real time and call off an attack should that purport to violate principles of proportionality (in the IHL sense) and distinction.[133] If the drone is acting as a swarm, to what extent should direct human involvement/participation be present in order to provide oversight in terms of distinction and proportionality compliance? Again, one might draw analogous conclusions to that of more general fully autonomous systems. [134] While there may be a sense of 'losing humanity' further to a view taken by Human Rights Watch in respect of fully autonomous systems,[135] the same counter-critiques pronounced by Roscini with respect to more 'general' fully autonomous weapons are equally apt in this instance and will be transposed accordingly to the present discussion.[136]

First, the swarm in general terms may be operating far away from civilians eg on the high seas—a purpose for which, a recent test by the US Navy confirms that the swarm is fully apt.[137] Secondly, and it is here that the present authors take a slight issue with Roscini's conclusion regarding autonomous weapons, in that they are inherently unlikely to be motivated by self-preservation or revenge.[138] Certainly, while the swarm is not motivated by revenge, its *raison*

[131] ibid.
[132] ibid.
[133] ibid.
[134] ICRC Rep (n 102) 44–47.
[135] Roscini (n 121).
[136] M Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified', (2014) 90 *International Law Studies, US Naval War College* 308–40, 310. The author notes, 'Only human beings can be inhuman and only human beings can deliberately choose not to comply with the rules they were instructed to follow. To me, it seems more reasonable to expect (and to ensure) a person who devises and constructs an autonomous weapon in a peaceful workplace to comply with IHL than a soldier on the battlefield or in a hostile environment'.
[137] Roscini (n 121); Atherton (n 5). See also Bishop (n 23).
[138] ibid.

d'etre is premised on the survival instinct of protecting fellow members within that swarm which, while not revenge *per se*, is something tangibly similar. And at this stage one could heed to Roscini's caution that sympathy and remorse may not come so easily to an autonomous system, or in our case, the swarm. Equally, would the swarm be able to balance the proportionality values of loss of life and military advantage? With respect to autonomous weapons, Roscini views this discussion as a fluid consideration within which, the pre-programming could account for all counter variables.[139]

However, and in terms of the distinction and proportionality parameters (accepting that the use of UAVs are IHL compliant) should the actions of the swarm (from a purely theoretical perspective, taking into account artificial intelligence (AI) advances) be held to a higher level of accountability? While the swarm may very well be pre-programmed, in a similar way to a soldier embarking on first deployment it is only through combat 'experience' that the swarm would become battle hardened and more perceptible through its AI advancement. To lower the legal threshold would be clearly undesirable and unpalatable, however, from a strictly theoretical perspective the logical inference is that the more combat experience the swarm has accrued the more likely it is both strategically and also legally compliant.

In sum, the compliance with IHL, or lack thereof, by a swarm (again in relation to Roscini's conclusions *vis-à-vis* general autonomous systems) is predicated on the fundamental concept that the recourse to drone swarms are not inherently unlawful (there is no sense that the swarms are equipped with indiscriminate weapons). However, there is clearly a sense of duty on the swarm operators or indeed programmers (in the event the swarm is fully autonomous) to take precautions so that if the target package is not militarily viable, the attack must be suspended if the swarm is in doubt of civilian presence, or indeed cease completely if surrender ensures.[140]

5. Conclusion

The article as a whole has sought to explore and shed light on a relatively neglected area within the literature by examining the extent to which, drone swarms are capable of complying with both *jus ad bellum* and *jus in bello* parameters. Within this broad overall remit, the article has focused its attention on specific areas contained in both the *jus ad bellum* and *jus in bello* in order to draw out the areas of tension (in terms of non-compliance) caused by the swarm's inherently unique behaviour. Within the confines of the *jus ad bellum* the article notes that should the swarm 'decide' to 'neutralise' the attacker of one of its members, providing such action fulfils the necessity and proportionality criterion, such action would be lawful. More problematic, however, and this

[139] Sassòli (n 136).
[140] Roscini (n 121).

is something which, will require further scholarly scrunity whether the Swarm engages in some form of anticipatory or interceptive defensive action. This action is not necessarily unlawful *per se*, however, it raises questions as to the exact threshold required for defensive measures by the swarms in order for them to fall within this somewhat elastic area of self-defence. Potentially, a neutralised drone within a swarm could satisfy the requirement, and one would also have to adopt a more permissive view of self-defence that a non-territorial attack can of course generate the lawful invocation of Article 51.

Usage or recourse to drone swarms is not inherently unlawful from a strict IHL perspective. However, the Swarm be it acting fully autonomously or semi-autonomously must have full regard to ensuring that the manner in which it engages the target and the selection of the target itself remains within the strict parameters of IHL. Given the progress being made in drone and swarm technology, and the rapid strides taken in deploying such advances to the conflict zone, one is made to believe that a scenario like the above is highly likely. As in the case of a State, there is also a clear sense of duty cast on the swarm operators or indeed programmers to take all necessary precautions to ensure that if and when the target package is perceived as not being militarily viable, (eg civilian presence of civilians) any intended attack be suspended. Simply put, the compliance with IHL, or lack thereof, by a swarm[141] is predicated on the fundamental concept that the recourse to drone swarms are not inherently unlawful, as one cannot take the position that the swarms are invariably equipped with indiscriminate weapons. Extending liability, interesting though it may be, beyond the swarm operator, and indeed programmer, is problematic. One could argue[142] that other categories of persons may also be liable (*eg*, the inventor or architect of the system and technicians who maintain them). Would, however, there be any beneficial distinction between a technician of a swarm as opposed to a technician of a non-autonomous/conventional tactical unit? Does the technician who does not correctly attach the missiles to a fighter jet, for example, or incorrectly 'services' nuclear weapons, then incur liability for IHL breach as a result of missile malfunction? If the weapon is inherently lawful, and is programmed as such, then failure to 'service' the weapon does not change its lawfulness although admittedly, it may affect its ability to comply with IHL. The authors contend, at least in the confines of this Article that such extension of liability makes no difference, and is also undesirable (the liability should and must remain with the operating state).

[141] Roscini's conclusions *vis-à-vis* general autonomous systems. See Roscini n 121.
[142] The authors are grateful to this helpful suggestion made by the anonymous reviewer.