

SWARM ROBOTICS

TECHNICAL AND OPERATIONAL
OVERVIEW OF THE NEXT
GENERATION OF
AUTONOMOUS SYSTEMS

MEREL EKELHOF & GIACOMO PERSI PAOLI



UNIDIR UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all the Institute's activities. This project is part of the Security and Technology Programme, which is funded by the Governments of Germany, the Netherlands, Norway, and Switzerland. UNIDIR and the authors would like to express sincere gratitude to the sponsors. The authors also wish to thank all the subject matter experts who participated in interviews and the focus group for their rich and invaluable input. The authors wish to thank, in particular, Vincent Boulanin for providing a background paper on swarming technologies and the peer-reviewers Magnus Egerstedt, Martin Hagström and John Matsumura for their comprehensive and constructive feedback. The views expressed in this report are the sole responsibility of the individual authors.

ABOUT UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or its sponsors.

CONTENTS

EXECUTIVE SUMMARY	1
1 INTRODUCTION	5
1.1 Method and approach.....	7
1.2 Purpose and structure of this report.....	8
2 COMMAND AND CONTROL	9
2.1 Command and Control in military operations.....	12
2.2 Swarms in the context of Command and Control.....	17
3 DECONSTRUCTING THE SWARM	21
3.1 Mass.....	25
3.2 Diversity.....	26
3.3 Collective and collaborative behaviour.....	26
3.4 Intra-swarm communication.....	27
3.5 Autonomy and decentralization.....	28
4 CONTROLLING THE SWARM	30
4.1 Commanding the swarm.....	31
4.2 Control architectures.....	34
4.3 Internal swarm coordination.....	39
4.4 Combined methods and alternative approaches.....	41
5 TRADE-OFFS	42
5.1 Framework of technical attributes.....	43
5.2 Balancing competing attributes.....	44
5.3 Other factors influencing the C2 approach.....	46
6 OPERATIONALIZING THE SWARM	48
6.1 Swarms in conflict.....	49
6.2 Limitations and challenges.....	53
7 MOVING FORWARD	57
BIBLIOGRAPHY	61
ANNEX	71

ABOUT THE AUTHORS



MEREL EKELHOF is the lead researcher of the AI/Autonomy Portfolio at the Security and Technology Programme at UNIDIR. Before joining UNIDIR, she was a PhD candidate at the VU University Amsterdam and an adviser to the Government of the Netherlands on issues related to autonomous weapons. Her recent work has focused on artificial intelligence and autonomy, military operations, targeting, and international law. She presents her work to and regularly engages with governments, humanitarian organizations, military services, intergovernmental organizations, research institutes, the media and non-governmental organizations. She is a NATO (Joint Force Air Component) certified targeteer and holds a PhD in Law and an LLM in Law and Politics of International Security from the VU University Amsterdam.



GIACOMO PERSI PAOLI is the Programme Lead for Security and Technology at UNIDIR. His expertise spans the science and technology domain, with emphasis on the implications of emerging technologies for security and defence. His recent work has focused on arms control, technology horizon scanning, artificial intelligence and cybersecurity. Before joining UNIDIR, he was Associate Director at RAND Europe, where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He served for 14 years as a warfare officer in the Italian Navy and has been extensively engaged in small arms and light weapons research in support of United Nations processes. He holds a PhD in Economics from the University of Rome and a master's degree in Political Science from the University of Pisa.

ABBREVIATIONS AND ACRONYMS

C2	Command and Control
C3	Command, Control and Communications
CARACaS	Control Architecture for Robotic Agent Command and Sensing
CCW	Convention on Certain Conventional Weapons
CODE	Collaborative Operations in Denied Environment
DARPA	Defense Advanced Research Projects Agency
DCIST	Distributed and Collaborative Intelligent Systems and Technology
GGE	Group of Governmental Experts
IED	Improvised Explosive Device
LAWS	Lethal Autonomous Weapons System(s)
NATO	North Atlantic Treaty Organization
OFFSET	Offensive Swarm-Enabled Tactics
R&D	Research and Development
SCAR	Strike Coordination And Reconnaissance
SOP	Standard (or Standing) Operating Procedure
T&E	Test and Evaluation
UNIDIR	United Nations Institute for Disarmament Research
V&V	Verification and Validation



EXECUTIVE SUMMARY

There is significant growing interest in many research laboratories and government agencies in developing **swarms of robotic systems** that have the ability to **coordinate their actions** to work collectively towards the execution of a **shared goal**. Working as a group, the swarm can perform both simple and complex tasks in a way that a single robot would be incapable of. Each robotic unit within the swarm can be considered an **autonomous member** that reacts according to internal rules and the state of the environment. Nevertheless, it is precisely this ability of robots to autonomously make decisions (individually or as a group) that raises concerns among the international community.

In 2014, governments began international discussions regarding emerging technologies in the area of Lethal Autonomous Weapons Systems (LAWS) under the auspices of the United Nations Convention on Certain Conventional Weapons (CCW). In this context, swarms have been discussed – albeit marginally. **Concerns about swarms being deployed as (lethal autonomous) weapons** have been raised by various States and civil society actors. During the meeting of the High Contracting Parties to the CCW in 2017, civil society actors released a fictional video illustrating their concerns about the proliferation of swarms and their possible use by malicious actors to conduct mass lethal attacks on individuals.

While it is not clear whether States share this concern, States at least recognize that in future scenarios, it would be unlikely that offensive measures would consist of a singular system. Instead, they would consist of swarms of such systems with complementary abilities. **Robotic swarms are not yet operational**, and the technology is rather brittle, but **the prospect of swarms is very real**. Swarms could be used for intelligence, surveillance and reconnaissance operations; perimeter surveillance and protection; distributed attacks; overwhelming enemy air defences; force protection; deception; search and rescue operations; countering swarms; and dull, dirty and dangerous tasks. As a result, the international community is grappling with questions about how – if at all – robotic swarms could be responsibly, lawfully and safely used in future conflicts.

One of the key issues in relation to both swarms and LAWS revolves around the meaning and operationalization of concepts such as “human-machine interaction” and “human control”. As expressed in the Chair’s summary of the 2016 CCW Meeting of Experts, in future scenarios **“where swarms of LAWS act as force multipliers, it would be unclear how meaningful human control**

could be maintained over the use of force”. As the CCW Group of Governmental Experts on LAWS enters two crucial years during which it will – among other activities – examine and develop aspects of a normative and operational framework on emerging technologies in the area of LAWS, understanding the direction in which research and development is progressing in this field is of utmost importance.

This study supports and informs these deliberations by examining the implications of swarm robotics for human-machine interaction. This report provides analysis of the various approaches to human control over swarms: (1) human-machine interaction by means of **command**, (2) a combination of human-machine and machine-machine interaction through the design and use of specific **control architectures**, and (3) machine-machine interaction resulting from the design and use of specific intra-swarm **cooperation methods**. In addition, it puts concepts of human control in the context of military decision-making, thereby introducing a framework of command and control, within which concepts such as human-machine interaction and human control can be further discussed, analysed and developed. The findings of this research are relevant for a wide variety of key stakeholders, including policymakers, military organizations, diplomatic communities, technical communities, academia, the private sector and civil society organizations.

Existing swarms – in the civilian and military domain – are either under development or still in a testing and demonstration phase. Past and ongoing projects have demonstrated, primarily, that **swarms are capable of conducting specific (narrow) tasks** (forming shapes, flying in formation, going to and searching or mapping an area, patrolling a perimeter, protecting a boundary). Swarms can thus be considered an emerging technology and, as such, may serve as a useful case study to discuss approaches to human control.

The main challenges in operationalizing swarms in a military context relate to the design and implementation of appropriate human-machine and machine-machine interactions. Researchers and developers have taken numerous approaches to injecting human involvement into a swarm. Human involvement or control in the context of swarming typically refers to either command, control or coordination:



Command: What orders do humans give? (Relates to the human-machine relationship.)

While swarms are expected to, for the most part, operate autonomously, they do not operate in a vacuum or without instructions. **Robotic swarms ultimately operate at the direction of human decision makers.** These commands may come in various forms, including pre-programmed sets of behaviour or high- or low-level commands.



Control: Which control architectures determine task distribution within the swarm? (Relates to the machine-machine relationship.)

After human-issued commands, the swarm relies on algorithms for formation, monitoring, spacing, flight path, task distribution, target identification and more. These algorithms or, as they are also known, **control architectures, determine the task distribution within the swarm.** For example, commands can go to one robot that acts as a central controller, but they may also go to several squad leaders or the entire swarm ensemble.



Coordination: How does the swarm execute those tasks? (Relates to the machine-machine relationship.)

After humans have provided the swarm (or specific units within the swarm) with commands and control architectures have determined how the commands will be distributed, **the swarm has to coordinate its collective behaviour and the assigned tasks.** How the swarm actions those assigned tasks depends, in part, on the coordination method. Examples include leader-follower (one robotic unit is the leader and the other robots act as followers), and consensus algorithms (individual robots communicate to one another and converge on a solution through voting or auction-based methods).

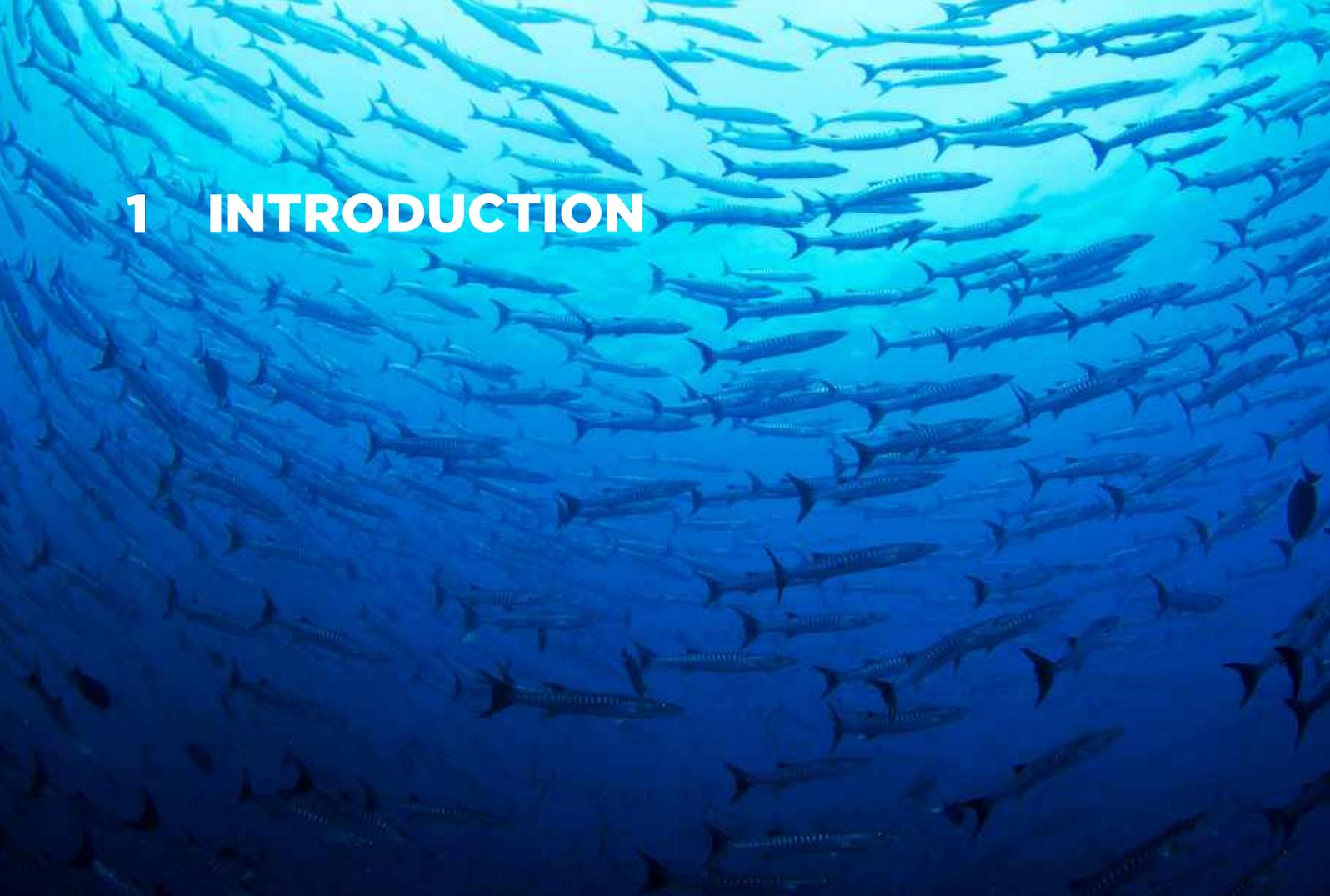
There is currently a dearth of studies investigating how humans can effectively command, control and coordinate swarms, and how to exercise effective and responsible levels of human involvement over swarms remains a nascent area of research in swarm robotics. There are many similarities between discussions about human control of LAWS and of swarms. However, swarms may further complicate the discussion for two reasons.

First, debates about **human-machine interaction** in the area of LAWS have focused primarily on the relationship between a human operator and a – or at least a limited number of – LAWS. When there is only a single vehicle (or a limited number of vehicles), traditional forms of control are possible. However, for swarms, **direct control of individual robotic units is both impossible and counterproductive.** For swarms, it is necessary to rely on algorithms for formation, monitoring, spacing, flight path, task distribution, target identification and more. Therefore, for human involvement to remain effective, it must shift increasingly to the swarm as a whole.

Second, besides human-machine interaction, swarms inevitably engage in **machine-machine interaction.** The **individual robots interact with other robots in the swarm to achieve a task** and, in so doing, collective behaviour may arise. While this report shows there are different approaches to designing command, control architectures and cooperation methods that help mitigate

some of the challenges that swarms raise, there seems to be no general method that explains the relationship between individual rules and (desired) group behaviour. Some may argue that machine-machine behaviour in swarms inevitably means there is no human control. While this may be true in some circumstances, it is not an inevitable consequence of swarming technology.

As the international community continues discussions on LAWS in 2020 and 2021 and will focus on the further development and operationalization of the guiding principles, **the role of human decision-making will undoubtedly remain one of the core issues.** By drawing on near-term technologies, such as swarms, and related command and control models in deliberations about human control and human-machine interaction, the international community can move to develop a more comprehensive understanding of how control may or may not be exercised in military practice – now and in future operations.



1 INTRODUCTION

Increasing advances in robotics are transforming many industries, from manufacturing to health care, agriculture, toys, transportation and warehouse management. Similarly, developments in robotics are changing the way in which wars are fought. Individually, robotic systems provide significant advantages, such as extended range, greater resilience and more dangerous concepts of operations than possible or acceptable with personnel or manned systems. Collectively, robotic systems may present even more disruptive changes to the conduct of military operations.

There is significant growing interest in many research laboratories and government agencies in developing networks of robotic systems that have the ability to operate autonomously in a collaborative manner. Comparisons can be made to animal species; for example, an individual ant is a rather simple entity (not very bright and almost blind),¹ but a colony of ants operating in a team can exhibit extraordinarily complex behaviour, like building impressive formations, foraging, killing and moving large prey.² While robot swarms differ from animal

¹ Still, an insect can still be considered a rather complex creature (it can process a lot of sensory input, respond to stimuli, interact with other creatures and make decisions on the basis of a large amount of information). Nonetheless, the complexity of an individual insect seems to be insufficient to explain the complexity of the collective behaviour of insect colonies. Bonabeau et al. (1999, 6).

² Kordon (2010, 145–74).

swarms in important ways,³ the underlying idea of simple rules guiding individual units leading to aggregate swarming behaviour of a collective group applies to both.

Swarm robotics, as a field of multi-robotics, considers large groups of robots that, typically, operate autonomously and coordinate their behaviour in a decentralized manner. Working as a group, the swarm can perform both simple and complex tasks in a way that a single robot would be incapable of, thereby giving robustness and flexibility to the group.⁴

Research and Development (R&D) in the area of swarm robotics is still relatively young. Most developments are experimental, and operationalization typically comes in the form of testing and simulation in laboratories or other structured and controlled testing environments. Even though swarms have not reached the operational stage yet, they are anticipated to bring significant advantages to war-fighting.⁵ One of those advantages is greater mass. Swarms of robotic systems could, for example, converge in an attack on a missile site by saturating or overwhelming the missile launchers by their sheer number, or they could cover a large area to search for targets. But swarms bring more than just greater numbers to the battlefield. Simply having a lot of systems is not the same as having a swarm of collaborative systems. To harness the full potential of swarming – such as improved coordination, intelligence, flexibility, speed and resilience on the battlefield – swarms need the ability to autonomously coordinate their actions between units within the swarm and respond to a changing environment.

Nevertheless, it is precisely this ability of robots to autonomously make decisions that raises concerns among the international community. In 2014, governments began international discussions regarding emerging technologies in the area of lethal autonomous weapons systems (LAWS) under the auspices of the United Nations Convention on Certain Conventional Weapons (CCW). While lethal swarms are not yet operational, there is no reason to believe that swarms cannot be armed with lethal weapons. Already, there have been reports of small robots armed with explosives designed to explode on impact, small arms, or even flamethrowers.⁶ Concerns about swarms being deployed as (lethal autonomous) weapons have been raised by various actors. For example, at the 2016 Meeting of Experts on LAWS, it was suggested that “in future scenarios, it

³ Robot swarms can leverage a mix of communication methods (explicit and implicit); robot swarms may consist of heterogeneous agents; swarm security is a larger concern in robotic swarms; while animal swarms' behaviour evolves, robot swarms are designed and, ultimately, operate at the direction of a human to perform a task. Scharre (2014b, 25–26).

⁴ Navarro & Matía (2013, 1). The main idea of swarm intelligence is the modelling of a system as a self-organized group of autonomous individuals that interact with one another and their environment. Flasinski (2016, 66).

⁵ For example, Kania (2017) explains: “The [Chinese People’s Liberation Army] recognizes the disruptive potential of these techniques, which could be used for saturation assaults ... to overwhelm the defenses of high-value targets, including perhaps U.S. fighter jets or aircraft carriers.” For more examples, see McMullan (2019); Scharre (2014b).

⁶ National Academies of Sciences, Engineering, and Medicine (2018, 12–13).

would be unlikely that offensive measures will consist of a singular system. Instead, swarms of such systems with complementary capabilities may carry out attacks".⁷ And in the video *Slaughterbots*, which was released during the meeting of the High Contracting Parties to the CCW in 2017, civil society actors warned about the mass proliferation of swarms of armed drones to malicious actors.⁸

Like LAWS, swarms raise questions about human control, responsibility, reliability and predictability. Direct control of individual units in a swarm would be not only counterproductive but, most likely, impossible. To harness the full potential of the swarm and allow for appropriate levels of human involvement, some argue that swarms will require new Command and Control (C2) models.⁹ Others, however, argue that appropriate human involvement is contradictory to a swarm; assuming that a swarm is inherently unpredictable, humans would be unable to control its behaviour in a way that is appropriate or meaningful.¹⁰

1.1 METHOD AND APPROACH

The United Nations Institute for Disarmament Research (UNIDIR) is undertaking research to enhance knowledge and facilitate dialogue among a broad range of stakeholders (including States, technical communities, academia and the private sector) on the implications of increasingly intelligent and autonomous systems for human control. This research report is framed in the broader context of "human control" – a rather undefined but key concept in the context of the Group of Governmental Experts (GGE) on LAWS and in the Secretary-General's disarmament agenda (action 29). The approach taken in this research is to look at the introduction of swarming technologies in military operations from a C2 perspective, seeking to draw from current theories¹¹ and practices regarding C2 and identify where the risks and uncertainties lie when applied to robotic swarms.

Given the early stages of R&D and limited (prototype) use of swarms for military purposes, studying operational practices of swarm deployment and lessons learned was not a possibility at the time of writing. As a result, this research, undertaken between October and December 2019, is based on the review of existing literature on the subject, supplemented by a total of 21 key informant interviews held in advance of a focus group comprising 15 subject matter

⁷ Informal Meeting of Experts on Lethal Autonomous Weapons Systems (2016, para. 68). In para. 67, it is also mentioned that "the unpredictability of LAWS could be exacerbated in situations where multiple systems or swarms of systems interact".

⁸ Future of Life Institute (2017). It is, however, unclear from the video whether the individual units communicate or exhibit any form of collaborative behaviour.

⁹ Scharre (2014b, 6). Or as explained by Ilachinski (2017, xix), "the operationalization of swarms ... will require the development of new [concepts of operation]".

¹⁰ Interview with anonymous expert, 16 October 2019; Informal Meeting of Experts on Lethal Autonomous Weapons (2016, para. 68).

¹¹ Theories captured in military doctrine, but also theories of various machine-machine and human-machine relationships developed in the private sector and military R&D.

experts in the area of swarming technology, human-machine teaming and C2. The focus group, held on 3 December 2019 in Washington, DC, was designed to explore, discuss and evolve the meaning of control in relation to swarm technologies, especially in the context of military C2. It focused on building bridges between the technical and military domain and identifying implications of weaponized swarms.

1.2 PURPOSE AND STRUCTURE OF THIS REPORT

The purpose of this research report is to support and inform ongoing discussions about emerging technologies in the area of LAWS and related concepts, such as human-machine interaction. The findings of this research are relevant for a wide variety of key stakeholders, including policymakers, military organizations, diplomatic communities, technical communities, academia, the private sector and civil society organizations. Against this backdrop, this report examines approaches to command, control and coordination in the field of swarm robotics.

It first sets out, in **Chapter 2**, the context within which weapons, including swarms, will be used and humans will exercise control. Understanding this contextual framework of C2 in military decision-making is relevant for discussions about concepts such as “meaningful human control” and “human-machine interaction”, in relation to LAWS as well as swarms.

Chapter 3 introduces the defining features of a swarm from a technical perspective, while **Chapter 4** explains how command, control and coordination are considered and applied in the context of ongoing swarm R&D. **Chapter 5** introduces the concept of trade-offs between different types of swarms and their characteristics, based on a number of technical attributes.

As swarm robotics is still a relatively young discipline and no (military) swarms are, as yet, operational, **Chapter 6** elaborates on potential military applications, challenges and vulnerabilities in operationalizing swarms. **Chapter 7** concludes this report by providing relevant considerations for moving forwards in the context of ongoing GGE on LAWS discussions.





2 COMMAND AND CONTROL

Since governments began international discussions on LAWS in the context of the CCW in 2014, maintaining control over emerging technologies in the area of LAWS has been one of the main objectives. As there seems to be agreement among States that all weapon systems should be subject to some form of human involvement, States and civil society actors have come up with various notions to capture that objective, such as “meaningful human control”,¹² “appropriate levels of human judgment”,¹³ and “human-machine interaction”.¹⁴ Ever since these concepts were first introduced, various participants (States, non-governmental organizations, research organizations and academia) have made attempts to further specify them. Despite these attempts, there seems to be no shared understanding of what these concepts mean and how they may be operationalized in practice.¹⁵

Conceptualizations of the human-machine relationship and concerns about the loss of meaningful human involvement are not limited to the development and use of singular LAWS. As expressed in the Chair’s summary of the 2016 CCW Meeting of Experts, in future scenarios “where swarms of LAWS act as force multipliers, it would be unclear how meaningful human control could be maintained over the use of force”.¹⁶ As the international community is grappling with new conceptualizations of the human role in relation to LAWS and swarms, it is worthwhile to consider what concepts and models related to control may already exist in the context of military operations.

The concept of C2 is a central aspect of military decision-making, yet it has received little attention in diplomatic discussions about human-machine interaction. In particular in the context of LAWS, control is regularly associated with the “select” and “attack” functions of the weapon. Concepts such as “meaningful human control” are often aimed at ensuring that operators and commanders exercise control over the operation of a weapon or the final decision to attack a target. While operators and commanders may certainly make critical decisions about the use of force, this focus is too limited because, in practice, various individuals may exercise different forms of control at various junctures in the decision-making process and at various command levels in the

¹² Article 36 (2013).

¹³ US Department of Defense (2017).

¹⁴ Group of Governmental Experts on Lethal Autonomous Weapons Systems (2019, 3).

¹⁵ UNIDIR (2014) examined what may be understood by “meaningful human control”, its strengths and weaknesses as a framing concept for discussions on autonomy and weapon systems, as well as other conceptual and policy-oriented approaches that address concerns about the weaponization of increasingly autonomous technologies.

¹⁶ Informal Meeting of Experts on Lethal Autonomous Weapons Systems (2016, para. 68).

organizational structure.¹⁷ In other words, “while individuals certainly pull the triggers or drop the bombs, the underlying causes of a large portion of collateral damage deaths and injuries may lie at the organizational level.”¹⁸

To gain a better understanding of the implications of swarms, a closer examination of the organizational context within which C2 is operationalized and weapons are deployed is necessary. The next sections first establish a common set of working definitions for key concepts related to C2. After discussion of the military-operational context within which humans and technologies collaborate, swarms will be introduced in the second section.

2.1 COMMAND AND CONTROL IN MILITARY OPERATIONS

C2 in the military domain is distributed and context dependent. It can be exercised at various levels by an arrangement of personnel and through a range of procedures, facilities, communications and equipment employed by a commander in planning, coordinating and controlling operations.¹⁹ As such, control can be perceived as something that is part of a chain of C2, rather than something that is only applied in relation to military capabilities such as LAWS or swarms. The general purpose of C2 is to focus the efforts of the individuals, organizations and resources in the chain of command towards the achievement of tasks, objectives or goals.²⁰



Command and control is not an end in itself, but it is a means toward creating value.”

SOURCE: ALBERTS & HAYES (2006, 32–33).

2.1.1 Concepts and definitions

Fundamental to understanding a C2 structure is a shared understanding of terms. This can be a challenge, since multinational or combined operations – similar to multilateral deliberations such as the GGE on LAWS – are often complicated by the use of a shared language that is subject to diverging interpretations.²¹ Although the term “command and control” is widely used, the terms (both individually and collectively) may mean different things to different

¹⁷ Ekelhof (2019b, 347–48).

¹⁸ Crawford (2013, 314).

¹⁹ NATO (2004, 2–7); NATO (2016a); US Air Force (2016); US Joint Chiefs of Staff (2010, 4, 77).

²⁰ Alberts & Hayes (2006, 32).

²¹ Cathcart (2012, 261).

communities.²² Nevertheless, the following definitions of “command” and “control” are broadly recognized:

Command: The authority vested in an individual of the armed forces for the **direction, coordination and control** of military forces.²³ Commanders can assign missions or tasks to subordinate commanders or forces under his or her command.²⁴

Control: The authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, that encompasses the responsibility for **implementing orders or directives**.²⁵ Control can refer to the authority delegated to the operational commanders to direct the forces assigned (**operational control**), but it may also refer to **tactical control**, which is the detailed and usually local direction and control of movements or manoeuvres necessary to accomplish missions or tasks assigned.²⁶

Thus, “command” can be considered as perceiving and deciding (the “what”), whereas “control” can be associated with implementing orders by communicating decisions, (organizing to) carry them out and monitoring and assessing the outcome to feed back into command (the “how”). This continuous decision-making cycle can be considered the C2 loop.²⁷

²² Many countries simply merge the two terms; these terms, merged or individually are, in turn, associated with a number of related concepts or definitions. UK Ministry of Defence (2017, 10).

²³ Similar in North Atlantic Treaty Organization (NATO), European Union and United Nations definitions. NATO, EU & UN (2015, 35).

²⁴ NATO, EU & UN (2015, 140, 179) includes further definitions: “operational command ... The authority granted to a commander to assign missions or tasks to subordinate commanders, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as the commander deems necessary.” And “tactical command ... The authority delegated to a commander to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority.”

²⁵ Similar in NATO and the European Union, but no recognized United Nations definition. NATO, EU & UN (2015, 46).

²⁶ Operational control is recognized in NATO and United Nations definitions but not recognized in the 2015 European Union glossary. The definition of tactical control is only officially recognized in the NATO glossary. NATO, EU & UN (2015, 140, 179).

²⁷ Kometer (2007, 59).

LEVELS OF COMMAND AND CONTROL

The standard view shared by most major military forces is that there are three main levels of command, each of which may exhibit various forms of control. While it may not always be practical or possible to draw a clear distinction between the different levels of command, there is a difference in terms of nature and function.²⁸ First, there is **strategic** command, which typically refers to the overall direction and coordination of assigned forces and the provision of advice to and from political authorities at the national and international level. At this level, the political aim is translated into military objectives, including allocating means – and restrictions that apply to the use of those means – without specifying in detail how they should be deployed. Second, there is **operational** command, which employs forces to attain strategic objectives in a theatre of operations through the design, organization and conduct of operations. In other words, the operational level translates the broad strategic-level objectives and guidance into concrete tasks for tactical forces to achieve. Third, there is **tactical** command, which directs the specific use of military forces in operations and, as such, implements the operational-level plan.²⁹ This level may come into direct contact with the parties to the conflict and is concerned with the methods of deployment and operation of units, platforms, individual personnel or weapon systems.³⁰

The distinction between strategic, operational and tactical command is recognized in most doctrines – albeit sometimes in slightly different terminology. For example, the current command structure in the Russian Federation consists of three levels: strategic, operational and brigade, where brigades are mobile, permanent-readiness units that, similar to units at the tactical command level, may come into contact with the parties to the conflict. However, Russian views regarding strategic, operational and tactical or brigade levels of command may be somewhat different from Western States. Whereas Western States typically define these levels by echelon size, the Russian system defines them by the unit's scope of mission. For example, a brigade is usually considered as acting at the tactical level, but when a brigade is a determining factor (a "war winner"), it could be considered a strategic asset.³¹

2.1.2 Centralization and decentralization

Within the hierarchical organization, commanders decide how to balance centralization and decentralization. For example, C2 in the Indian Armed Forces is “underpinned by a philosophy of centralised intent and decentralized execution – this enables freedom of action and initiative. The spirit in the concept remains to describe the ‘what’ and not specify the ‘way’.”³²

However, in accordance with the applicable rules of engagement, commanders may also decide to delegate tasks and authorities to lower levels (subordinate commanders) and, as such, pursue a more decentralized approach to control. This will give the lower levels more freedom of decision-making and the ability to respond to situations as they unfold (while all actions of lower levels must be in compliance with the commander’s intent and the constraints provided). Decision-making may involve a wide range of decisions, including weapons deployment, the course of action, and the desired end state.

How to balance centralization and decentralization may vary across commanders, services,³³ and countries. For example, whereas both the US and Russian processes are “commander-driven”, Russian commanders are said to be more involved with the order process than US commanders; this can be illustrated by Russian commanders developing the course of action, instead of the staff (in an iterative process between various command levels).³⁴ North Atlantic Treaty Organization (NATO) doctrine explains that the primary role of the staff is to assist the commander in timely decision-making by acquiring, analysing and coordinating information and, most importantly, presenting the essential information with a recommendation for decision-making.³⁵ And China uses a theatre-specific command structure that is, in turn, under the strategic and overall control of the Central Military Commission (the military branch of the national Government).³⁶

Last, the balance between centralization and decentralization may also depend on other factors, such as missions, physical environments, available information, political sensitivities of the operation and more. Each operation typically has a unique C2 structure, designed during the planning to match the requirements of the operation. It may be necessary to adapt the C2 structure to changing circumstances or to reflect lessons learned. Thus, C2 approaches may be

³² Integrated Defence Staff (2017, 36).

³³ For example, it is not uncommon for control to be relatively decentralized in the army, while in the air force, control may be more centralized (e.g. owing to there being fewer assets). In the air force, the doctrine of centralized control and decentralized execution has become dominant in controlling air operations.

³⁴ Bartles & Grau (2018, 51).

³⁵ NATO (2017, 5-1 to 5-2).

³⁶ Sugiura (2017, 17–18).

different depending on purposes and circumstances, and they may change over time.³⁷

2.1.3 The distributed nature of military decision-making

C2 should not only be assessed through the actions and decisions taken by commanders but should rather be seen as a distributed process through which various staff – as well as systems, organizations and even technologies – influence, make and execute decisions.³⁸

Decisions made by one link in the chain almost definitely will affect the choices or limit the decisions of others in the chain. For example, if – on the basis of information provided by analysts and perhaps technologies – a targeteer³⁹ nominates a particular target (system) for further development (while disregarding potential others), this influences the targets that may be presented to the commander for inclusion in the target list. Military decision-making is thus based on a division of labour, where various individuals make decisions within a context that is created by other individuals, relying on intelligence gathered and assessed by others and acting under the command of their superiors.⁴⁰



Commanders exercise control through processes and structures that enable them to verify the execution of their intent. **The staff often exercises control on behalf of the commander.**

SOURCE: NATO (2017, 5-4).

³⁷ NATO (2017, 5-5).

³⁸ Ekelhof (2019a).

³⁹ A “targeteer” is an individual who has completed the requisite training and guides the joint targeting cycle by conducting tasks such as analysing, developing and nominating targets; preparing target folders; and weaponeering.

⁴⁰ Schulzke (2013, 204).

THE THIRD C: COMMUNICATIONS

For effective C2 to be accomplished, there is a need for two-way communications. Without communications, commands could not be passed to the appropriate persons or platforms, and control would be impossible without some form of feedback. Given the importance of communication, it is regularly added as a third element to C2: Command, Control and Communications (also known under the abbreviation C3). While this report focuses on C2, it is critical to acknowledge the importance of reliable communications in allowing for C2 to be operationalized at all.

Military communications technologies come in large numbers and many forms, ranging from traditional high-frequency radios to complex and elaborate satellite communications systems.⁴¹ In hostile environments, communications can be fragile. They can be jammed or destroyed by adversaries, but even without external influence in the form of malicious attacks, communication may not always be reliable (it can be interrupted and intermittent) or possible (e.g. underwater systems). Recognizing that secure and reliable communications are key requirements for effective C2, militaries are continuously looking at optimizing their communications networks and technologies.

2.2 SWARMS IN THE CONTEXT OF COMMAND AND CONTROL

Swarming is still in its infancy, and R&D is mostly experimental. Therefore, how to effectively and responsibly command and control robotic swarms after deployment is an open question. Even the most cutting-edge R&D projects struggle to develop an effective human-machine relationship, in particular as swarms grow larger.⁴² Controllability of a swarm's collective behaviour depends on a number of factors, including:

- **The size of the swarm:** As the number of robotic units in a swarm increases, human control must increasingly shift to the swarm as a whole.

⁴¹ Stratcore Group (2020).

⁴² Interview with anonymous expert, 21 October 2019. The expert explained that there is still a long way to go before humans can intuitively interact with robotic swarms close to 250 units (as is pursued under the Defense Advanced Research Projects Agency [DARPA] Offensive Swarm-Enabled Tactics [OFFSET] project).

- **The flow of information:** Without information and the ability to communicate across the units in the swarm, the ability to steer the swarm towards some desired performance will be complicated.
- **The autonomous capabilities of each system:** For example, aerial vehicles that are flown in an autopilot mode relieve the operator from manual flying tasks, allowing different forms of control.
- **The design of the system:** For example, a vehicle without a steering wheel does not have the same capabilities as a vehicle with one and, as a result, requires different forms of control.⁴³

In general, as the number of robotic units in a swarm grows, it becomes increasingly difficult for humans to control every individual unit. Therefore, for human control to remain effective, that control must shift increasingly to the swarm as a whole. How to exercise effective and responsible human control over swarms remains a nascent area of research where “no one size fits all”.

2.2.1 Swarms at the tactical level

From the perspective of military C2, it could be said that – even though the decision to deploy may be taken at the operational or even strategic levels – a swarm operates at the tactical level.

Before tactical-level deployment, human decision makers will formulate mission objectives, gather intelligence,⁴⁴ analyse and develop potential targets and decide which weapon(s) to use and under which circumstances and conditions. Once these decisions have been made, operational and tactical-level planning has been completed, and the swarm has been deployed by a tactical (human-issued) command, it could be argued that the swarm itself exercises tactical control over its own elements during operation.

In this context, tactical control means the detailed and usually local direction and control of movements or manoeuvres necessary to accomplish the missions or tasks assigned. Ultimately, the aim of swarming would be that the swarm is capable of executing these lower-level tasks (determining movements and manoeuvring) to achieve its mission without traditional forms of human control.

This raises questions about how swarm behaviour fits within existing military C2 structures. According to some experts, new technologies, specifically robotic swarms, will require new C2 models.⁴⁵ Because “command and control structures emerge from complex interactions between people, structures, technology and

⁴³ Egerstedt (2011, 158).

⁴⁴ Swarms can also be used to contribute to these tasks. One of the most anticipated near-term applications of robotic swarms involves their use as extended sensors to gather intelligence about specific areas. This is further explained in Chapter 6.

⁴⁵ Scharre (2014b, 6). Or as explained by Ilachinski (2017, xix), “the operationalization of swarms ... will require the development of new [concepts of operation]”.

processes”,⁴⁶ changes and advances in technology can be expected to impact the C2 model. Nevertheless, some argue that “technology has not changed the fundamental principles of command and control”.⁴⁷ Chapter 4 takes a closer look at approaches to C2 in swarm robotics. Before that, some clarifying notes on language are in order.

2.2.2 Military and technical language

It should come as no surprise that the term “command and control” in relation to swarm robotics is less common in civilian R&D than in the military domain. However, even in some military swarming projects, the term “C2” is deliberately avoided, in part because the term is rather disputed.⁴⁸ The same applies to the term “control”. Some experts argue that the aim is not to control the swarm in a traditional sense (e.g. providing digital commands to individual units) but rather to command the swarm (e.g. have the individual units collaborate with one another in accordance with the higher-level commander’s intent).⁴⁹

While there seems to be no shared definition of the terms among experts, it seems that, generally, “command” is related to the input or instructions provided by human operators or commanders (human-machine interaction),⁵⁰ while “control” is related to the swarm algorithms that are executing the orders through the movement, motions and coordination of the swarm (design of the swarm architecture). As such, the interpretation of C2 is not dissimilar to that in military operations.

2.2.3 Mathematical and natural language

Humans think and interact in a language that is not easily codified in mathematical language. At the same time, algorithmic-based machine behaviour is based on mathematical language that is difficult to translate appropriately into natural language.⁵¹ Translating complex mathematical concepts into natural language (and vice versa) can thus introduce a range of complications and inadequacies. Natural languages are significantly less precise in describing the characteristics and inner functioning of swarm algorithms.⁵² Therefore, natural language may be useful in introducing technical concepts, but there is a limit to what it can describe about the underlying computational

⁴⁶ UK Ministry of Defence (2017, 35).

⁴⁷ Kometer (2007, abstract). Kometer continues that new technologies have, nonetheless, altered the way in which humans perform their jobs, and even the jobs they perform.

⁴⁸ Interview with anonymous expert, 21 October 2019.

⁴⁹ Scharre (2014b, 38); interview with anonymous expert, 21 October 2019.

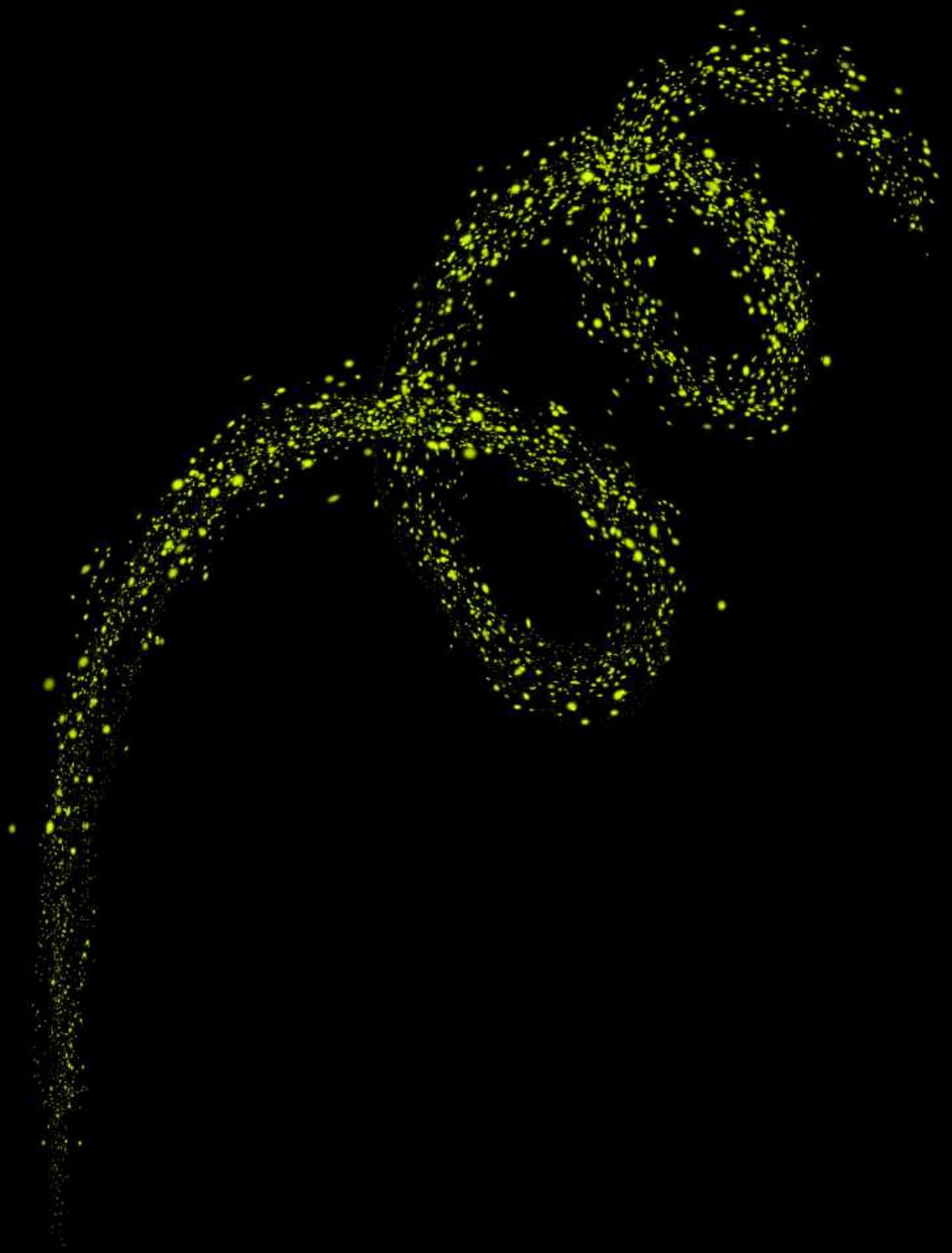
⁵⁰ Commands can also be provided or passed along by robots if information is disparate. Regardless, it seems that (high-level) commands are, at least initially, designed and provided by humans.

⁵¹ Multidisciplinary fields concerned with interactions between computer and human (natural) language include natural language processing and human-computer interaction.

⁵² Personal Communication with anonymous expert, 9 December 2019.

algorithms. As such, the next sections are not intended to give a precise description of the swarm architectures and algorithms but rather to introduce defining features and general concepts of control architectures in the context of swarming.

.length; c-
b.push(a[
function h(
user_logged
place(/+(?
) , b == [],
0 == n
c =



3 DECONSTRUCTING THE SWARM

Swarming as a concept is not new. Swarms can be found, first and foremost, in nature. Examples are schools of fish (foraging and defending against predators), colonies of wasps (nest building), bird flocks (foraging and migration) and termite colonies (building massive and complex structures).⁵³ In these swarms, individuals do not need sophisticated knowledge to produce complex behaviours and, typically, there is no group leader that guides all the other individuals in accomplishing their goals. One individual is not able to accomplish its task without the rest of the swarm. As such, the knowledge of these natural swarms is distributed across all the individuals.⁵⁴

However, swarming is not limited to natural phenomena. It is also a long-standing military tactic. Swarming as a military tactic occurs when several units converge to attack a target from multiple axes in a deliberately structured, coordinated way.⁵⁵ This type of swarming has occurred throughout military history, ranging from the behaviour of horse archers in the fourth century to swarm-like capabilities that simultaneously target multiple vulnerabilities, devices and access points in cyberspace.⁵⁶

The swarms discussed in this paper are robotic swarms. Robotic systems, such as the Predator aircraft and counter-IED robots, are already used in military operations. Individually, these systems allow militaries to protect their own forces, extend their range on the battlefield, and increase situational awareness and persistence. Collectively, swarms of robotic systems have the potential for even more disruptive changes in military operations.⁵⁷ They may bring mass back to the battlefield, for example the use of large numbers of robots to expand sensing and striking capabilities. Nonetheless, as will be explained in this chapter, swarming is more than just having greater numbers of robotic systems.

Swarm behaviour is based on the use of local rules and relatively simple robots that, when organized in a group, can perform complex tasks in a way that a

⁵³ The *Macrotermes* species builds complex nests composed of cone-shaped outer walls that often have ventilation ducts, brood chambers, thin horizontal lamellae supported by pillars, cooling vents, a royal chamber, a thick-walled protective bunker with holes through which workers can pass, and more. Bonabeau et al. (1999, 4).

⁵⁴ Navarro & Matía (2013, 1).

⁵⁵ Arquilla & Ronfeldt (2000, 5); Edwards (2005, xvii).

⁵⁶ Edwards (2005, xvii); Fortinet (2018).

⁵⁷ While some experts consider swarms of robotic systems to be the next step in a continuum of robotic R&D (like the Predator drone), one expert pointed out that swarms could be considered the opposite of the Predator drone in that one Predator is said to require a lot of personnel to be operational (according to Noorman (2014, 818), it can take up to 168 people to keep a Predator in the air for 24 hours), while large numbers of robotic systems operating in a swarm would require only one person to be operational. Interview with anonymous expert, 9 October 2019.

single robot would be incapable of.⁵⁸ Much like discussions about LAWS, artificial intelligence and autonomy, there is no single or agreed definition of a swarm. The meanings of these terms seem to be far from settled, both within the international community and the private sector, academia and technical communities. While conscious of this technical and political context, for the purpose of this report, we propose the following working definition of swarms: **multi-robot systems within which robots coordinate their actions to work collectively towards the execution of a goal.**

Such a definition can be a useful foundation for further debates; however, discussing definitions in a political body like the CCW – of which the purpose is to ban or restrict the use of certain types of weapon – is rather contentious. As such, it may be useful to discuss and define swarms by reference to a number of defining features. The next sections will further examine these features: mass, diversity, collective and collaborative behaviour, intra-swarm communication, and autonomy and decentralization.

WHAT IS A ROBOT?

Robotic systems are enabled by the integration of three key capabilities: sense, decide, act.

Sense. Robots need sensors to gather data about the environment. For small robotic systems, these are typically video cameras and some kind of navigation sensor, like GPS. Larger systems might use computer-intensive sensors like lidar.

Decide. Robots need to make sense of that data and turn it into purposeful plans and actions. To do so, they need a suite of computer chips, sensing software and control software. Together, these technologies form the “brain” of the system.

Act. The decisions of the robots are exerted in the real world through their end-effectors and actuators.⁵⁹

⁵⁸ Navarro & Matía (2013, 1). The main idea of swarm intelligence is the modelling of a system as a self-organized group of autonomous individuals that interact with one another and their environment. Flasinski (2016, 66).

⁵⁹ Boulanin & Verbruggen (2017, 11–12).

3.1 MASS

As the etymology of the term indicates, swarms are regularly associated with a large group of insects, people or robots.⁶⁰ The simplest description of a robotic swarm is that there are many robotic units and only a few people involved in controlling them. However, there is no magic number and, in theory, swarms may vary from as few as two units to thousands of units.⁶¹

Significant attention is given to projects that intend to develop the largest swarm possible. In 2014, Harvard University's 1,000-robot swarm was reported as being the largest robot swarm ever.⁶² According to the *Harvard Gazette*, "the vast scale of this swarm is a milestone in itself."⁶³ Until then, only a few robot swarms had exceeded 100 individual units because of the difficulties related to coordinating such large numbers (as well as the cost and labour involved in producing the robots⁶⁴). In 2017, a private company in China set a world record by performing a light show with 1,108 miniature drones that, allegedly, had self-repair capabilities and so-called independent thought, demonstrated by units executing their own landing when falling out of sync with the group or failing to achieve the intended objective.⁶⁵

Even though large swarms have been promoted regularly in the context of, for example, light shows, it is not always clear what the technology behind the group behaviour is (whether the units are centrally controlled, have pre-programmed flight paths or exhibit any coordinated or collaborative behaviour). As explained by Scharre, "a swarm with 10 more individual drones isn't necessarily better. What matters are the things you can't see. It's the algorithms that govern the swarm behavior."⁶⁶

While it could be said that "quantity has a quality of its own", the optimal size of a swarm will ultimately depend on the swarm's capabilities and the mission. For example, a large swarm could be particularly useful for a saturation attack or for a search mission over a large area. However, a large swarm may have a large footprint and draw a lot of attention, which would be detrimental for a stealthier

⁶⁰ Nearly all experts consulted in the process of this research referred to size as one of the characteristics, although many pointed out that describing a swarm as a large group of robots was insufficient.

⁶¹ Some experts argue that a swarm can be as few as two systems, while others argue that a swarm consists of a minimum of 40 robots. National Academies of Sciences, Engineering, and Medicine (2018, 12–13).

⁶² Woo (2014).

⁶³ Perry (2014).

⁶⁴ Researchers at Harvard discovered a new manufacturing process allowing them to print microdrones cheaply, effectively and without errors by printing them by the sheet. Global Guerillas (2012); Perry (2014).

⁶⁵ Irvine (2018). At the time, Chinese media quoted military experts who highlighted that this technique could be used with mission payload modules mounted on the small drones and that it might be integrated into weapon systems. Liu (2017). Also see Kania (2017).

⁶⁶ Feng & Clover (2017).

mission.⁶⁷ At the same time, a larger swarm could mean additional challenges and risks resulting from algorithmic limitations that complicate the coordination of such large numbers, risking collisions, occlusions and loss of communication.

3.2 DIVERSITY

While swarms are regularly portrayed as a large number of exact copies of robotic units (homogeneous),⁶⁸ a robotic swarm can be heterogeneous. A swarm may consist of a variety of dissimilar units with a mix of properties and tasks assigned. Similar to social insect colonies, a single unit may not perform all tasks but rather specialize in one or a set of tasks according to its capabilities.⁶⁹ For example, the Defense Advanced Research Projects Agency (DARPA) Offensive Swarm-Enabled Tactics (OFFSET) programme envisions a combination of unmanned aircraft systems and unmanned ground systems to accomplish missions in complex urban environments.⁷⁰ Similarly, a European Union initiative called Roborder uses aerial, water surface, underwater and ground vehicles in its autonomous border surveillance system that are said to be capable of operating in swarms.⁷¹ Heterogeneity can be achieved by equipping similar robots with different payloads (e.g. different sensors or weapons), and they may be assigned different tasks depending on their capabilities. However, heterogeneous swarms are said to be more difficult to implement than homogeneous swarms.⁷²

3.3 COLLECTIVE AND COLLABORATIVE BEHAVIOUR

Experts agree that for swarms to be different from simply large numbers of individual robots, they need to exhibit collective behaviour that involves collaborating among individual units and with the environment.⁷³ In this context, some experts make a distinction between swarming and teaming.

Teaming, sometimes referred to as collaborative autonomy, can be illustrated by hunting wolf packs or a basketball team playing a game. Each individual has an understanding of the mission and a mental model of their roles; they each

⁶⁷ Kallenborn (2018); interview with anonymous expert, 30 October 2019. For example, as illustrated by the White House lockdown on 26 November 2019, the way in which a flock of birds appears on a radar screen can be similar to the “look” of a small aircraft. While it has not been confirmed that the lockdown was caused by a flock of birds, it is one of the possible explanations for the “slow-moving blob” that was seen on radar. Cohen et al. (2019).

⁶⁸ Examples can be found in drone light shows, but homogeneous agents are also common in natural swarms. The arms control advocacy video *Slaughterbots* demonstrated a fictional scenario in which swarms of thousands of homogeneous microdrones could be deployed.

⁶⁹ In a social insect colony, this division of labour among workers, whereby different activities are performed simultaneously by groups of specialized individuals, is perceived as being more efficient than if all tasks were performed by unspecialized individuals. Bonabeau et al. (1999, 2).

⁷⁰ DARPA (2019). The Distributed and Collaborative Intelligent Systems and Technology (DCIST) Collaborative Research Alliance too creates heterogeneous swarms in a wide range of missions and environments. DCIST (2020).

⁷¹ Roborder (2019).

⁷² Defense Science Board (2016, 85).

⁷³ Sometimes this is referred to as “self-organization”. Ilachinski (2017, 106).

know the plan that they are supposed to execute to achieve the common goal.⁷⁴ While some argue that having a group of individual robots execute a program (for both individual and group plans) should be considered teaming or multi-robot systems, rather than swarming,⁷⁵ others argue that differentiating between teaming and swarming is unhelpful and unnecessary or, at least, unclear and confusing.⁷⁶ Regardless, it is generally agreed that one of the key characteristics of a swarm is that simple interactions between units can induce complex collective behaviour.

Considering this, many swarm demonstrations, such as Intel's drone light show during the 2018 Winter Olympic Games,⁷⁷ may not be considered "true" swarming if the robots are unaware of their counterparts, such as when the choreography of the drone is pre-planned and the individual robots simply follow their pre-programmed flight paths. These robots exhibit behaviour that seems collective but is certainly not collaborative. Nevertheless, in these large groups of robots there may be some limited awareness of other units if the robots are deconflicting to avoid collisions. Without knowing the algorithms behind the group behaviour, distinguishing between swarms, teams (multi-robot systems) and large groups of non-cooperative robots can be a challenge.⁷⁸

3.4 INTRA-SWARM COMMUNICATION

To achieve collaborative behaviour, some form of communication to allow for information exchange among the robots is necessary. Communication may take different forms, both explicit and implicit. Some common technologies for explicit communication are wireless signalling over Bluetooth, Wi-Fi, radio, lidar,⁷⁹ infrared or a mix of methods. Nevertheless, while these methods may work well in a controlled environment, such as a laboratory, they may not be optimal methods in an operational setting. Particularly in a military environment, explicit communication is vulnerable to attacks, such as spoofing, jamming or hacking.⁸⁰

An implicit form of communication is, for example, co-observation. In a school of fish, there is no explicit communication, but the fish coordinate their behaviour by observing neighbouring fish.

⁷⁴ An example of teaming or collaborative autonomy projects in a military context is the DARPA Collaborative Operations in Denied Environments (CODE) project. This project is discussed in more detail in Chapter 4.

⁷⁵ Kolling et al. (2015, 1); interview with anonymous expert, 16 October 2019.

⁷⁶ Interview with anonymous expert, 8 October 2019; interview with anonymous expert, 30 October 2019.

⁷⁷ It was a world record in terms of the number of drones deployed (1,218 drones), but the swarm had zero percent decision-making autonomy. Each individual drone was commanded by an external computer. Intel (2018).

⁷⁸ This is further complicated by the lack of stringent definitions.

⁷⁹ Lidar, a combination of laser and radar, produces an image by scanning a very high repetition rate laser rangefinder over a scene to produce a three-dimensional map. Department of Defence Science and Technology (2019).

⁸⁰ This is further discussed in Chapter 6.

Another implicit communication method is the modelling of behaviour. In a sports team, the individual players have a mental model of what the other players on the team will be doing, because they are “running the same play”.⁸¹ This is not dissimilar to military tactics, where battle drills are used to train teams to execute coordinated manoeuvres with limited or no explicit communication among them.⁸²

3.5 AUTONOMY AND DECENTRALIZATION

Each robotic unit within the swarm can be considered an autonomous member that reacts according to internal rules and the state of the environment. The algorithm used to program a swarm is distributed, meaning that the algorithm of the swarm runs separately on each individual robot in the swarm.⁸³ Swarms are typically not centrally controlled but are instead based on decentralized, cooperative behaviours between multiple units. In other words, the behaviour of a swarm is a collective property of the combined decisions of otherwise autonomous robots.⁸⁴

While swarms such as flocks of birds may give the impression that centralized control is directing the overall movement and direction of the flock, evidence strongly suggests this is a decentralized activity, where each bird acts according to its own local perceptions of what nearby birds are doing.⁸⁵ However, even though natural swarms seem to have no central controller, robot swarms cannot operate without any instructions. **They ultimately operate at the direction of human decision makers.** That does not mean that humans control the behaviour of each individual robot; instead, they exercise control over the swarm as a whole.

Theoretically, by increasing the autonomy of each robot, the operator’s workload would be reduced as increased robot autonomy could reduce the number of tasks the operator needs to accomplish.⁸⁶ This allows for decentralized control; for example, a human operator decides which target should be attacked and authorizes the swarm as a whole to engage, while the swarm coordinates which of its units should carry out the attack according to a list of parameters, such as proximity and payload. While decentralized control

⁸¹ Interview with anonymous expert, 8 October 2019.

⁸² Scharre (2014b, 24).

⁸³ In swarm robotics, the terms “decentralized” and “distributed” are sometimes used interchangeably. However, in some cases, the term “distributed” relates to the tasks (division of labour) within the swarm, while the terms “centralized” and “decentralized” relate to the coordination within the swarm. For example, a system could be both distributed and centralized when a centralized coordinator receives the commands and then distributes the tasks among the individual units. Interview with anonymous expert, 11 November 2019.

⁸⁴ Ilachinski (2017, 90).

⁸⁵ Ilachinski (2017, 117).

⁸⁶ Nevertheless, it may also add significantly more complexity to the system as a whole, making it much harder to certify as safe. Also, decentralized models may come with both increased autonomy and increased neglect times, which may, in turn, exacerbate a loss of the operator’s situational awareness and promote complacency and skill degradation. Cummings (2015, 980, 989).

has various benefits (e.g. scalability, robustness, speed), the outgrowth of decentralized swarms may have radical implications for C2 structures.



4 CONTROLLING THE SWARM

Human involvement or control in the context of swarming typically refers to (1) **command** (i.e. the human-machine relationship: What orders do humans give?), (2) **control** (i.e. a combination of human-machine and machine-machine relationships: Which control architectures determine task distribution within the swarm?) and (3) **coordination** (machine-machine relationships: How does the swarm action those tasks?). Because swarms can exhibit self-organized emergent behaviours that arise in complex adaptive systems, they may not be amenable to conventional design processes.⁸⁷ The following sections study existing approaches to command, control and coordination that are intended to facilitate these unique swarm behaviours, each with its own opportunities and challenges. These approaches to command, control architectures and coordination methods are not mutually exclusive; in practice, it is likely that a mix is applied.⁸⁸ As such, this chapter will conclude with a brief discussion of combined methods and approaches.

4.1 COMMANDING THE SWARM

While swarms are expected to, for the most part, operate autonomously, they do not operate in a vacuum or without instructions. As mentioned previously, robotic swarms ultimately operate at the direction of human decision makers.

Commands to a swarm may come in many forms. With manual control of each individual robot off the table, how do humans ensure that the swarm successfully accomplishes the tasks it is assigned? What are the types of command that operators may give to a swarm? And what kind of C2 relationships are most optimal for human-swarm interaction? These questions depend on multiple factors, including the control architecture, the coordination model, the communication methods, the human-machine interface, the information available to the operator and the context within which the swarm is deployed.

Certainly, there currently exist no validated schemes for scalable, flexible and adaptive human-machine interaction in the context of swarms.⁸⁹ Different approaches to commanding swarms are being explored. The next paragraphs will provide further details on existing methods to command swarms; these are examples and should not be considered a comprehensive overview.

⁸⁷ Ilachinski (2017, 223).

⁸⁸ Personal Communication with anonymous expert, 9 December 2019.

⁸⁹ Ilachinski (2017, 126).

4.1.1 Low-level commands

In the context of swarm robotics, designing the necessary (tactical-level) commands to ensure that the swarm behaves as desired may be incredibly complex. According to Ilachinski:

“The “devil is in the details” resides in designing an appropriate “language” that describes policy-orders in a way that is precise (read: mathematical) enough to yield unambiguous swarm behaviour, yet is “simple” enough to be understood by a human operator who may not be programming savvy”.⁹⁰

Currently, it is unreasonable to expect robots to be able to execute commands like “take that hill” or “establish air supremacy”.⁹¹ However, simpler, lower-level commands have already proven to work in swarm robotics, at least in R&D, testing and simulation. For example, a swarm could be commanded to “go to area B; once there, look for red things, and when you have found them, form a protective boundary around them”. Or “go to this location and take some pictures”. Currently, these commands require the specific programming of definitions of the individual elements, such as “red thing” and “protective boundary”. Particularly, low-level commands related to forming shapes, flying in formation, going to and searching an area, patrolling a perimeter or protecting a boundary are feasible with the current state of technology.

4.1.2 Higher-level intent

According to some, the ultimate aim in swarming is to have a decentralized swarm where robots react to their surroundings in accordance with a higher-level commander’s intent.⁹² Several projects are exploring possibilities to command a swarm by providing higher-level instructions, while delegating lower-level decision-making to the robotic units.⁹³ Rather than micromanaging actions on the swarm algorithm level, these projects aim to command a swarm by giving it a sequence of behaviours.⁹⁴ For example, in a firefighting scenario, high-level commands could be “isolate danger setting; secure perimeter; create path for first responder vehicles”.⁹⁵ It would be then up to the robots to collaborate with others in the swarm to understand and explain what it means

⁹⁰ Ilachinski (2017, 133).

⁹¹ Beal (2012, 15).

⁹² Scharre (2014b, 38).

⁹³ Raz et al. (2019, 1) suggest a “game theoretic machine learning C2” concept, where they introduce autonomy in the independent systems, which collaborate to accomplish the commander’s intent while remaining subordinate to their human operators or commanders. See also Cruise et al. (2018, 23–30); DARPA (2019).

⁹⁴ Interview with anonymous expert, 21 October 2019.

⁹⁵ Interview with anonymous expert, 21 October 2019.

to, for instance, “secure a perimeter”.⁹⁶ Determining the appropriate human-system interaction is an ongoing research question, and many open issues remain. In this context, conveying the commander’s intent to the swarm and from the swarm to the human supervisors is particularly challenging.

4.1.3 Behaviour selection

In swarms with behavioural control architectures (see Section 4.2.4), each individual robot has a pre-programmed set of behaviours in their internal library. While this is a specific design choice, it also influences the way in which humans command the system. Instead of giving low- or high-level commands, humans command the swarm to execute a specific pre-programmed behaviour.⁹⁷ By selecting a pre-programmed behaviour, the human acts as a switch. These types of command may be given (uploaded) before an operation or given or changed in real time. The latter presupposes that the operator can develop an understanding of what the different swarm behaviours look like and that inputs can be communicated to the swarm at the appropriate time.⁹⁸ Once the swarm has been instructed to execute a certain behaviour, humans rely on the autonomy of the swarm to deal with lower-level tasks such as movement, obstacle avoidance, and intra-swarm communication and coordination. Commands in the form of behaviour selection may also be based on perception, where the robots match their behaviour according to what they perceive in the environment.⁹⁹

4.1.4 Collaborative autonomy

Yet another, perhaps more collaborative, method to command a group of robotic units is by means of communicating specific plans. In DARPA’s Collaborative Operations in Denied Environment (CODE) programme, unmanned vehicles present recommendations for actions to the human supervisor, who may approve or disapprove those actions or direct the group to collect more data.¹⁰⁰ While CODE is regularly referred to as a swarm project,¹⁰¹ CODE’s project manager does not agree.¹⁰² Instead, CODE could be compared to a wolf pack or a basketball team, where there is a common plan distributed among the members of the group, each member of the group is highly

⁹⁶ This approach is explored in DARPA’s OFFSET project. Other projects that focus on higher-level commands in swarms are Crandall et al. (2017); Cruise et al. (2018, 23–30); Raz et al. (2019, 1). Interview with anonymous expert, 21 October 2019.

⁹⁷ See, for example, Bashyal & Venayagamoorthy (2008, 1–8); Kolling et al. (2012, 89–96).

⁹⁸ Kolling et al. (2015, 8).

⁹⁹ Interview with anonymous expert, 18 October 2019.

¹⁰⁰ Cooney (2015).

¹⁰¹ See, for example, Article 36 (2013, 3). According to FlightGlobal, CODE fits within DARPA’s larger vision of swarm robotics controlled by a single source. Giangreco (2018).

¹⁰² Interview with anonymous expert, 16 October 2019.

sophisticated, the group coordinates with minimal communications, and a human can review and influence the plan during the operation (in real time).¹⁰³

4.1.5 Setting parameters

While specific spatial and temporal limitations will vary, every military operation is limited in time and space to allow for coordination and deconfliction (e.g. to prevent duplication of effort and blue-on-blue engagements). In the context of swarms, these parameters may offer a way of control to decision makers. Even though these parameters may not directly influence the behaviour of the swarm, they may limit the time and space within which the swarm can operate, and they may indirectly affect the swarm behaviour from interaction with its environment.¹⁰⁴ Controlling a swarm's behaviour through setting parameters may, however, require militaries to adapt their thinking. When, for example, the US Air Force started testing its Perdix swarm (103 microdrones released from a canister in the back of military aircraft), a flight plan for each drone was requested. However, because these drones determine their own flight path in real time (adaptive formation flying), planners had to shift their thinking from "you need a flight plan" to "you need a box".¹⁰⁵

4.2 CONTROL ARCHITECTURES

Besides control through commands, swarm behaviour can be controlled by means of design choices. One way to exercise control by design is through a swarm's control architecture. Extensive research is being conducted on developing control architectures in centralized and, particularly, decentralized swarms. While traditional forms of control are possible over a single or a limited number of vehicles, for swarms of robotic units it is necessary to rely on algorithms for formation, monitoring, spacing, flight path, task distribution, target identification and more. These algorithms could be used for ten, a hundred or even more systems, making them – at least theoretically – highly scalable. Given the state of R&D, the most common architectures (executed through various algorithms) currently used for control *within the swarm* are centralized control, hierarchical control, ensemble-level control and behavioural control.

¹⁰³ Scharre (2018); interview with anonymous expert, 16 October 2019.

¹⁰⁴ Kolling et al. (2015, 8).

¹⁰⁵ McCullough (2019). Nevertheless, having a box within which to execute an operation is not unusual in military practice. For example, in a Strike Coordination And Reconnaissance (SCAR) mission, a fighter aircraft searches for targets in a specific geographic area with the purpose of finding and fixing targets for engagement by a designated strike aircraft. SCAR missions are conducted in an area (or "box") because certain targets may be known to exist in the area, but they have not yet been detected, located and identified. US Joint Chiefs of Staff (2014, I-4).

4.2.1 Centralized control

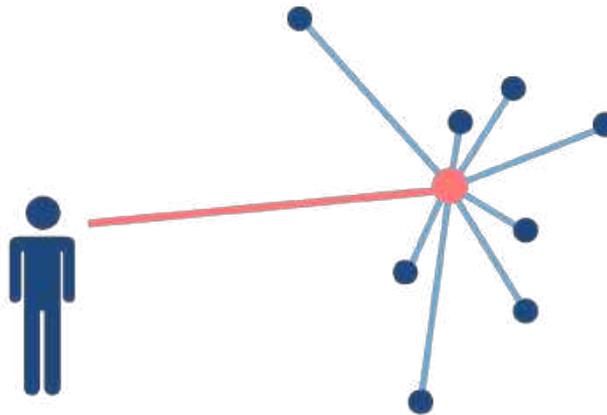


Fig. 4.1: in centralized control, the commands go to the centralized controller, which, in turn, distributes instructions to each individual robot in the swarm.

Centralized control is when a central controller, after receiving a command from a human operator, tasks each robotic unit individually (Figure 4.1). In this architecture, there is no collaboration between the units directly, except that which goes through the central controller.¹⁰⁶ While it is not unusual to have human operators conduct central controller functions, this would, arguably, no longer be considered a swarm.¹⁰⁷ In swarm robotics, the central controller is a robot that receives commands from human operators and processes and distributes these instructions to the various units of the swarm, while being an integral part of the swarm. This control architecture can be compared to air traffic control, where all coordination goes through the traffic control centre (e.g. monitoring, managing airspace, and issuing landing and take-off instructions) and the execution of specific tasks (e.g. executing manoeuvres and changing flight paths on the basis of higher-level instructions) is left to the pilots of the individual aircraft.¹⁰⁸

Given that an attack on the central controller could cripple the swarm as a whole, centralized control is relatively vulnerable. Regardless, it is possible to minimize vulnerability by designing for a succession of control if the central controller of the swarm is compromised. In this case, there is one central controller at a time, but if that robot is destroyed or damaged, the leadership is delegated to another robot. This delegation can, for example, be based on tail numbers (the robot with the lowest tail number will become the new controller) or positions (the robot that is operating at the highest altitude will become the new controller). That way, the swarm can continue its mission, because control is delegated if

¹⁰⁶ Nevertheless, individual units can be aware of one another without active collaboration.

¹⁰⁷ Expert discussion, focus group, 3 December 2019.

¹⁰⁸ In a way, air traffic control is also hierarchical in that there is typically not one controller. Rather, there are multiple controllers that hand off aircraft among themselves. Interview with anonymous expert, 9 October 2019.

the central controller is compromised.¹⁰⁹ Nonetheless, succession of control is only possible to robots with the required leadership capabilities.

4.2.2 Hierarchical control

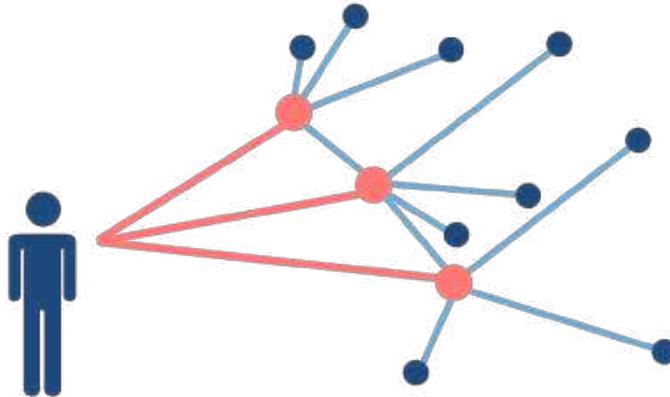


Fig. 4.2: in hierarchical control, the commands go to (one or) several "squad leaders", which, in turn, distribute instructions to the individual robots in their "squad".

When centralized control is not desirable (e.g. because it is too vulnerable) and transmitting instructions from a central controller to each robotic unit is not feasible (e.g. because the size of the swarm is too large, the bandwidth insufficient or the operational environment does not allow it), a human controller may transmit commands to several leaders in the swarm.¹¹⁰ The leaders then, in turn, communicate with the individual units in the swarm (e.g. via their neighbours). In hierarchical control architectures, individual robots may be controlled by several lower-level ("squad" level) agents, which are in turn controlled by higher-level controllers, and so on.¹¹¹ (See Figure 4.2.)

Communication through localized "squad leaders" may result in a more robust swarm that is less vulnerable to communications disruptions.¹¹² While this type of control architecture may also accelerate the speed of immediate reaction, the time needed to communicate instructions to one or several leaders in the swarm, which have to, in turn, communicate those instructions to the robots in their "squad", increases as the group size increases (e.g. to a hundred or a thousand robots). As such, this architecture is said to work particularly well in small groups.¹¹³

¹⁰⁹ Expert discussion, focus group, 3 December 2019.

¹¹⁰ Where there is only a single leader, the model would be best described as centralized control.

¹¹¹ Scharre (2014b, 38).

¹¹² Scharre (2014b, 38).

¹¹³ Interview with anonymous expert, 18 October 2019.

4.2.3 Ensemble-level control

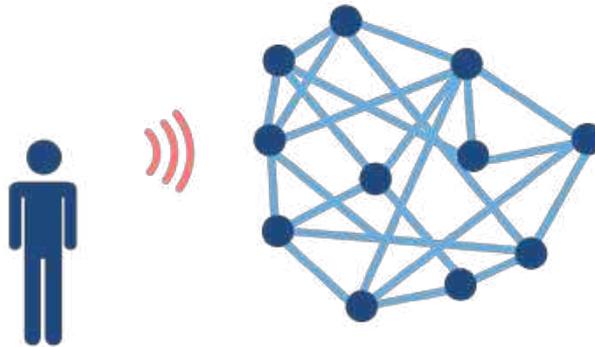


Fig. 4.3: in ensemble-level control, the commands are broadcast to the swarm as a single group, after which the individual robots make decisions on how to action that command.

While hierarchical control can be particularly efficient in coordinating behaviour among the various robots in the swarm, it is typically not as flexible, tolerant of errors or reliable as ensemble-level control. Ensemble-level control is a decentralized method that allows the broadcast of commands to a swarm as a single group, after which the individual robots make decisions on how to execute that command (Figure 4.3). Because there is no central controller or leader(s), there is no single point of failure.

Ensemble-level control can be combined with emergent coordination (discussed in Section 4.3.4), which allows this architecture to work well in operations with high levels of uncertainty. This type of control, however, also means that specific actions would not necessarily be predictable in advance.¹¹⁴ Ensemble-level control is said to be useful in finding solutions to complex problems and can work with low bandwidth between the different elements (or even without explicit communication between elements), making it less vulnerable to attack than centralized or hierarchical control.

¹¹⁴ Scharre (2014b, 40).

4.2.4 Behavioural control

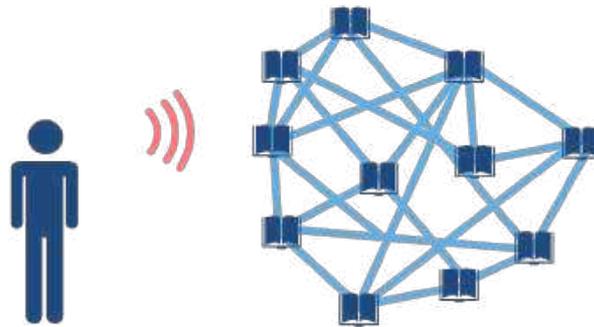


Fig. 4.4: in behavioural control, each individual unit has a pre-programmed library of behaviours. The human commands the swarm to execute a certain behaviour.

Another decentralized coordination model is behavioural control. In this architecture, a human can determine the swarm's behaviour by exercising control over how the units respond to the environment.¹¹⁵ Each robot has a library of behaviours, and operators command the system to execute a certain behaviour or, in other words, to run a certain program (Figure 4.4). For example, robots may be tasked to execute a search mission. They may be updating one another to optimize their behaviour (e.g. deconflict search areas) and, once they find the object of interest, their behaviour may change into tracking or even targeting.¹¹⁶ This method can be based on perception, for instance when real-time communication is not possible or desirable.¹¹⁷

Similar to ensemble-level control, this type of control allows for a more diverse and robust swarm than centralized or hierarchical control, because there is no single point of failure. Behavioural control differs from ensemble-level control in that actions may be more predictable because the behaviour of the swarm is based on a pre-determined library of behaviours. However, while ensemble-level control, in particular with emergent coordination, works well in operations with high uncertainty, behavioural control can become increasingly difficult to apply in complex missions and in unexpected situations that require behaviours that are not programmed.¹¹⁸

In a way, behavioural control can be compared to issuing Standard (or Standing) Operating Procedures (SOPs). SOPs are specific instructions that guide personnel in carrying out standard (routine) operations to ensure efficient, uniform and desired outputs.¹¹⁹ SOPs can be compared with the swarm's library

¹¹⁵ Interview with anonymous expert, 18 October 2019.

¹¹⁶ For an example of this type of control architecture, see DARPA CODE.

¹¹⁷ However, particularly in targeting missions, communication with a human operator may be required for legal, political or operational reasons. These military applications are further discussed in Chapter 6.

¹¹⁸ Ilachinski (2017, 133); Expert discussion, focus group, 3 December 2019.

¹¹⁹ They may apply to all sorts of operations, from peacekeeping to military and crisis response situations. See, for example, UNDP (2018); UNDPO (2016); US Department of the Army (2011).

of behaviours, prescribing the desired behaviour in specific situations. While it is impossible to predict how the environment or tactical situation will evolve during an operation, SOPs allow a certain level of predictability in responses.

4.3 INTERNAL SWARM COORDINATION

After humans have provided the swarm (or specific units within the swarm) with commands, and control architectures have determined how the commands will be distributed, the swarm has to coordinate its collective behaviour and action (execute) the assigned task(s). The following section explains some common approaches to facilitating internal swarm coordination (i.e. actioning decisions): leader-follower, consensus algorithms, utility functions and emergent coordination. While some coordination methods are more likely to be used in combination with specific control architectures (e.g. leader-follower in hierarchical control), they could, theoretically, be applied to each of the four architectures described above (i.e. centralized control, hierarchical control, ensemble-level control and behavioural control).

4.3.1 Leader-follower

The leader-follower model designates one robotic unit as the leader and the other robots as followers.¹²⁰ It is arguably the most well-known approach to swarm control and is most regularly used in centralized and hierarchical control models.¹²¹ This method is often used to control a swarm's formation, but leader-follower models can also be used for more complex tasks. For example, a single or a small number of robotic agents can be responsible for tactical planning by deciding which robot in the swarm performs which task, while working jointly with the human operator to define plans that meet operational goals. In this case, the human provides the operational goals and makes global decisions – for example, regarding locations and targets of interest – while the leader (in this case, the tactical planner) optimizes the trajectories of each robotic unit in the swarm.¹²² Rather than the other robots simply following the leader's trajectory, the leader can assign specific tasks to individual robots in the swarm.

4.3.2 Consensus algorithms

Another method to coordinate swarm behaviour – perhaps most common in ensemble-level control – is through consensus algorithms.¹²³ By means of consensus algorithms, the individual robots communicate to one another and

¹²⁰ See, for example, Xu et al. (2014).

¹²¹ Campobasso (2017, 2).

¹²² Cummings et al. (2011, 662–63).

¹²³ See, for example, Davis et al. (2016, 3801–08).

converge on a solution through voting or auction-based methods.¹²⁴ This model may have high degrees of decentralization, for example when robots negotiate among themselves which robot would be assigned which task, while each robot determines its own route.¹²⁵ Consensus-based models have been proposed for a number of swarm coordination problems – such as resource and task allocation and formation control – and allow for individual robots to determine not only their own role in the swarm but also that of other robots.¹²⁶

4.3.3 Utility functions

Another approach, presented in a NATO publication, is the use of utility functions as a method for the swarm to optimize its behaviour and choose the appropriate action. The swarm is given a high-level command (a goal in the form of a utility function), after which the swarm balances the costs and rewards of particular actions and pursues the action that is considered the most utile (with the highest reward). The swarm could be used, for example, to detect and identify possible threats (i.e. serve as an early detection or identification system), while using utility functions to relate all (individual) actions to a common goal, such as the minimization of damage to a ship from fast attack crafts launched from the shore.¹²⁷ Utility functions could also be thought of as generalizations of the consensus algorithm in that they both coordinate by means of capturing consensus phenomena as well as use a broader set of objectives, such as covering areas and patrolling perimeters.

4.3.4 Emergent coordination

When no explicit communication between the individual robots is possible, control may be feasible through emergent coordination. In natural swarms, emergent coordination arises naturally by individual swarm elements reacting to others (e.g. in a school of fish or a flock of starlings). In robotic swarms, individual units are engineered and, as a result, the capabilities of individual units are known (from their design). However, as soon as individual units behave as a collective entity through emergent coordination, predicting its behaviour becomes incredibly difficult.¹²⁸ Some experts compare emergent coordination to the behaviour of musicians in a jazz ensemble, where individual musicians coordinate by reacting to the behaviour of the other musicians in the group.¹²⁹

¹²⁴ Scharre (2014b, 38).

¹²⁵ Cummings (2015, 987).

¹²⁶ Davis et al. (2016, 3801).

¹²⁷ Fransman & Kester (2012). For more work on utility functions see Aliman & Kester (2019).

¹²⁸ Predicting the collective behaviour may only be possible in limited circumstances. Expert discussion, focus group, 3 December 2019.

¹²⁹ Interview with anonymous expert, 16 October 2019; interview with anonymous expert, 21 October 2019.

4.4 COMBINED METHODS AND ALTERNATIVE APPROACHES

While discussed separately, the above approaches to command, control architectures and coordination methods are not mutually exclusive. It is likely that there will be a mix of each applied in a single swarm. In other words, different methods and approaches to control (both human-machine and machine-machine relationships) may exist within the same system. For example, a swarm may use consensus-based models for data sharing but leader-follower models to determine its route. Or tactical coordination of a swarm could be performed through emergent coordination, while centralized agents could perform operational-level coordination and human controllers could make higher-level decisions.¹³⁰

In addition, whereas the above figures illustrate the human as separate from the swarm, recent developments in the area of swarming examine assigning a wider variety of roles to humans. Humans may command the swarm from outside, but they may also operate as teammates within the swarm, or they may be functioning as bystanders (only consulted by the swarm when it needs guidance). For example, Distributed and Collaborative Systems and Technology (DCIST) – a collaborative research alliance of the US Army Research Laboratory – is creating “swarms of humans and robots [that] will operate as a cohesive team”.¹³¹

¹³⁰ Scharre (2014b, 41).

¹³¹ DCIST (2020).



ATTRIBUTES MISSION INTENT

R&D

SOPHISTICATED

SPEED

INFLUENCE

SWARM

LIBRARY

CONTROL

PERFORMANCE

ARCHITECTURE

COMPONENTS

BALANCE

CONDITIONS

TECHNOLOGY

CORRELATIONS

RANKING

BEHAVIOUR

COMMAND



5 TRADE-OFFS

The combination of different approaches to command, control architectures and coordination models may create different opportunities and risks in different situations. Choices about control in relation to swarms therefore depend on the balance of competing attributes.¹³² For example, whereas in a saturation attack on enemy air defences resilience and speed may be the most important attributes, when using swarms to attack soft targets predictability of the swarm's behaviour may be considered more important than speed. Depending on the context of use, some control architectures may be considered more useful (or pose higher risks) than others.

5.1 FRAMEWORK OF TECHNICAL ATTRIBUTES

To get a better understanding, at least at the theoretical level, of such trade-offs, a framework of **technical attributes** can be used to characterize different architectures. These attributes include:

- **System resilience:** The ability to continue performing the assigned mission or tasks in degrading conditions (e.g. denied communications or unavailability of one or more swarm elements, for example due to technical failure or kinetic force)
- **Predictability of behaviour:** The degree to which the operator can predict in advance how the swarm will interpret instructions and implement a given task
- **Influence over behaviour:** The degree to which the operator maintains the ability to intervene and alter the behaviour of the swarm as a whole or of its individual components
- **Speed:** The speed at which commands provided by the human operator are processed and actioned by the swarm
- **Technological sophistication:** The level of technological sophistication of the system as a whole or of its individual components

The five technical attributes described above are not officially, or unofficially, endorsed by any community of practice involved in swarms R&D, but they are useful analytical tools developed for the purpose of this study.

The understanding of each control architecture developed through this research (Section 4.2), allows us to rank them for each attribute. This ranking is summarized in Figure 5.1, which illustrates how different architectures compare

¹³² Scharre (2014b, 40).

against one another. The scale used for each attribute is from lowest to highest, with the external edge representing the “best performing” architecture for each attribute. These rankings should be considered as relative and not absolute assessments of individual performance. These assessments are made under the assumption that all other conditions remain unchanged (e.g. size of the swarm is the same, environment is the same, conditions remain unaltered during mission).

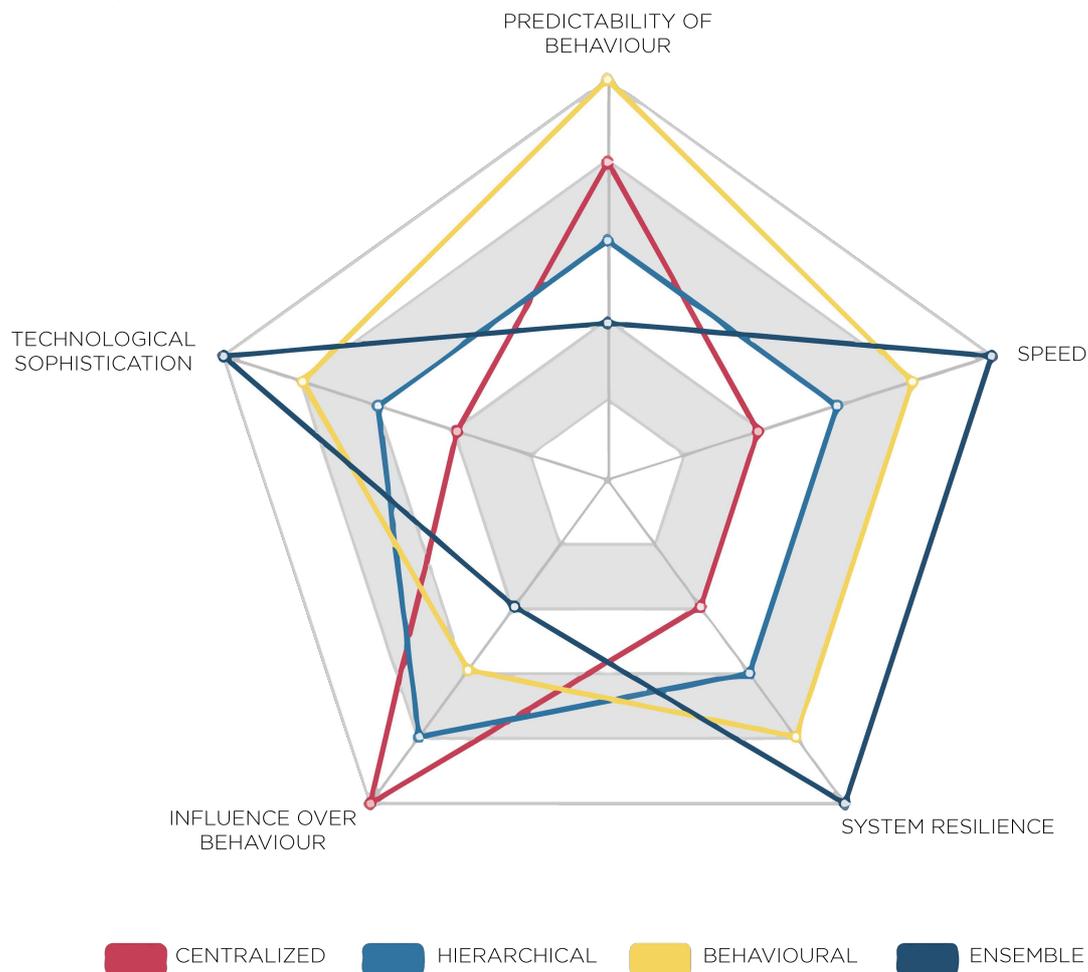


Fig 5.1: Technical attributes of control architectures in swarms.

5.2 BALANCING COMPETING ATTRIBUTES

Figure 5.1 shows that a perfect solution – one that is highly predictable, fast (in processing and implementing commands), highly resilient, technologically sophisticated (e.g. potentially able to conduct complex tasks) and easy to influence in real time – is not achievable with any single control architecture.

For example, **predictability** can be at odds with **technological sophistication**: as the system becomes more complex, it may also become increasingly difficult for a human to understand and explain its behaviour. Ilachinski argues this is “a fundamental tradeoff: either the [intelligent system] can achieve a given

performance level (e.g., it can play the game Go as well as, or better than, a human) or humans can be able to understand how its performance is being achieved".¹³³ The one exception in this case might be represented by behavioural control. By design, this control architecture is based on pre-programming behaviours and responses into a digital library uploaded on each element of the swarm, which is sophisticated enough to select the appropriate pre-programmed response in a given scenario (although this may become increasingly difficult to apply in complex missions and in unexpected situations that require behaviours that are not programmed). With this exception, it could be concluded that the simpler the control architecture, the more predictable the system is.

Similarly, technological sophistication appears to be linked with less influence over behaviour: more technologically advanced systems, operated through more complex control architectures such as ensemble-level or behavioural control, are meant to be less dependent on human input during the mission execution phase.

This leads to a parallel trade-off between **predictability** and **resilience**. Control architectures such as ensemble-level control operate on the basis that only the high-level intent or mission goal is set by the human operator, while the specific behaviour of the swarm is determined endogenously by the swarm itself. This could include reassigning tasks and roles to each swarm element in response to degrading conditions. By contrast, a centralized control architecture that relies on only one "synthetic brain" at a time (i.e. the swarm element with the role of central controller) is more predictable as the commands are given by the human at a more tactical level and passed to the rest of the swarm through a single iteration (i.e. human, to controller, to rest of the swarm). This comes at the cost of resilience and, typically, technological sophistication. As explained above, a centralized control architecture will be only as resilient as the percentage of its elements capable of performing central or tactical control roles.

Building on this concept, in addition to trade-offs it is possible to identify **positive (qualitative) correlations between attributes**. In general terms, more **technological sophistication** appears to be positively correlated to **speed** and **resilience**.

In terms of **speed**, more technologically complex architectures allow the human operator to interact directly with the swarm as a whole through either pre-programmed behaviours or by definition of intent or goal setting. This results in a shorter lag between the moment the command is given and the moment the swarm performs the assigned mission. Less complex architectures relying on one

¹³³ Ilachinski (2017, vi).

or more robotic controllers and a higher number of relatively simpler elements may result in longer time lags as (1) these architectures may require more frequent human interventions through commands and (2) each command has to be translated into specific instructions and transferred to each element of the swarm.

With respect to **resilience**, as mentioned in the discussion regarding predictability, more technologically sophisticated control architectures that are less reliant on a small number of swarm elements to perform control duties are typically more resilient to degrading environmental or operational conditions.

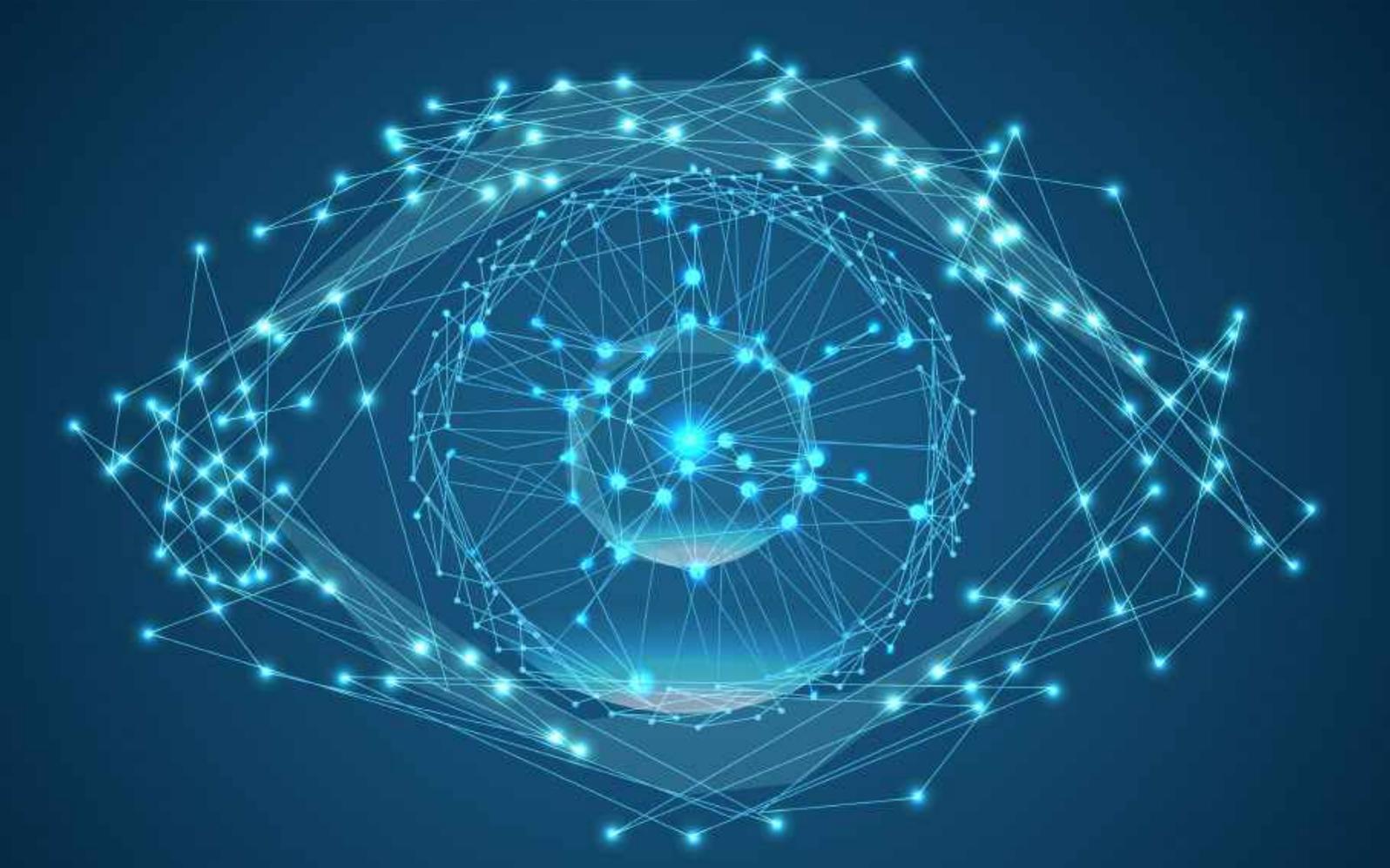
5.3 OTHER FACTORS INFLUENCING THE C2 APPROACH

How to determine the optimal C2 approach in a given situation will depend on the above attributes and trade-offs as well as on a set of critical, context-shaping factors. These shaping factors include, but are not limited to:

- **Environment:** Different environments present different risks, which is likely to be reflected in the choice of C2. For instance, while in urban environments swarms could be particularly useful (e.g. where forces cannot see over long distances and movement is channelized between buildings), these environments also present higher risks to civilians and friendly forces.
- **Situational awareness:** The greater the information available to decision makers before deployment of a swarm, the better they may be able to predict the swarm's behaviour in that particular environment.
- **Connectivity:** Connectivity both within the swarm and between the human and the swarm can be a challenge, in particular in hostile environments where there is a high risk of jamming, spoofing, hijacking or other electronic warfare.
- **Human-machine interface:** The interaction between the human and the swarm will depend on the tools available for communication through visual, aural and tactile means. In all cases, translating human commands into computer instructions (and vice versa) is a challenge.
- **Level of training:** Training and education is necessary for human operators and other decision makers in the chain of command to understand and adequately influence the behaviour and limits of the swarm.

- **Achievability:** Some attributes are more difficult to achieve and implement in practice. For example, a highly intelligent (technologically sophisticated) system that allows for highly interactive and advanced human-machine interaction is said to be harder to implement than a swarm that is based on simple, predefined rule sets and in which human-machine interaction is limited to a human giving the “Go” command.¹³⁴ As demonstrated by this report, the “ideal” swarm – possessing all the desired attributes – may not be achievable.

¹³⁴ Defense Science Board (2016, 85).



6 OPERATIONALIZING THE SWARM

Because existing swarms are either under development or still in a demonstration phase, distilling opportunities and challenges resulting from operationalizing swarms in military practice is complicated by the lack of practical examples. Past and ongoing projects have demonstrated, primarily, that swarms are capable of conducting specific (narrow) tasks (forming shapes, flying in formation, going to and searching or mapping an area, patrolling a perimeter, protecting a boundary). While these tasks may have useful military applications, being able to design, develop and test swarms in structured environments, such as a laboratory, is only the beginning. Deploying that same technology in an environment that is uncontrolled, unstructured and potentially hostile presents many more challenges. Challenges raised by the operationalization of systems that are developed and tested in static and structured environments, but of which the anticipated use is in dynamic and unstructured environments, are significant and, as of yet, unresolved.¹³⁵ Whether swarms can be effectively and responsibly operationalized in military operations will be dependent on a number of factors, including, but not limited to (1) the intended use of the swarms (military applications) and (2) specific limitations and challenges associated with operationalizing swarms in a military context.

6.1 SWARMS IN CONFLICT

Swarms are not designed in the abstract. Rather, they are developed with a specific intended use.¹³⁶ To gain a better understanding of the implications of military swarms on human control, studying the technology in isolation is of little use. While it is difficult to make reliable predictions of future swarm capabilities and uses in the context of military operations, swarm R&D and strategies provide insights into a range of looming applications of military swarms on and off the battlefield. Most prominently, swarm R&D focuses on intelligence, surveillance and reconnaissance missions; perimeter surveillance and protection; distributed attacks; saturating enemy defences; force protection; deception; dull, dirty and dangerous tasks;¹³⁷ and countering other swarms.

Whether independently or in coordination with other weapon systems, swarms may support critical areas of operational planning and tactical execution.¹³⁸ The applications discussed in this section are not argued to be legally, ethically and

¹³⁵ Ilachinski (2017, vi); Personal Communication with anonymous expert, 9 December 2019.

¹³⁶ Expert discussion, focus group, 3 December 2019.

¹³⁷ When discussing the types of task that robots are expected to “take over” from humans, it is common to refer to the three D’s of robotization: dull, dirty, dangerous. It is not uncommon to add more D’s, such as “dear” or “difficult”. Marr (2017).

¹³⁸ Kania (2017).

politically accepted; rather, this section aims to present emerging, anticipated or envisioned applications.

6.1.1 Intelligence, surveillance and reconnaissance operations

One of the most anticipated near-term applications of swarms involves their use as extended sensors to gather intelligence about specific areas, particularly in cluttered environments. These swarms may be tasked to search a defined area to, for example, find wounded soldiers or potential targets, or they may be used to map large areas.¹³⁹ Numerous projects are investigating the use of swarms for intelligence, surveillance and reconnaissance purposes. One project that has received significant attention is Perdix, designed and tested by the Strategic Capability Office of the US Department of Defense in partnership with the Naval Air Systems Commands. The project culminated in 2016 with the successful testing of a surveillance operation involving 103 Perdix drones launched from a combat aircraft at high altitude and at high speed.¹⁴⁰

The US Army Research Laboratory's DCIST research alliance also creates autonomous swarms for a wide range of missions in dynamically changing, harsh and contested environments, including search and rescue of hostages and information gathering after terrorist attacks or natural disasters.¹⁴¹ In the civilian realm, researchers from TU Delft, University of Liverpool and Radboud University of Nijmegen have developed a swarm of drones equipped with cameras that can be used to search unknown, indoor environments and find dummies (representing victims) in a disaster scenario.¹⁴²

6.1.2 Perimeter surveillance and protection

Another foreseeable application of swarm technology is for perimeter surveillance and protection. A European Union initiative called Roborder provides a good illustration of how swarms could be used for border patrol. Roborder uses aerial, water surface, underwater and ground vehicles in its autonomous border surveillance system that are said to be capable of operating in swarms.¹⁴³ Similarly, the CARACaS (Control Architecture for Robotic Agent Command and Sensing) project led by the US Office of Naval Research focuses on developing algorithms that enable a boat swarm fleet to identify and classify unknown vessels and coordinate among the swarm which unit should approach the unknown vessel, while communicating with the other units to conduct other

¹³⁹ See, for example, a search and rescue project conducted by researchers at Delft University of Technology (2019), and, in a military context, US and Indian collaborative efforts as well as DARPA's CODE project. Pandit (2019); Wierzbowski (2019a).

¹⁴⁰ Agence France-Presse (2015); Boulanin & Verbruggen (2017, 30–31).

¹⁴¹ DCIST (2020).

¹⁴² Delft University of Technology (2019); interview with anonymous experts, 16 October 2019.

¹⁴³ Roborder (2019).

tasks (assist in tracking and trailing or continue to patrol the area).¹⁴⁴ In May 2018, Chinese State media released a video demonstrating a swarm of 56 unmanned boats coordinating to avoid obstacles and manoeuvre into various shapes.¹⁴⁵

6.1.3 Distributed attacks

Swarms could potentially be used as weapon systems that autonomously distribute targets among themselves. In May 2019, the Chinese Zhuhai Ziyang drone company issued a statement that it had developed helicopter drones carrying proximity explosive mortar shells, grenades and machine guns that, enabled by swarming attack technology, could engage in coordinated strikes.¹⁴⁶ A month later, the Turkish company STM published a video claiming that its Kargu swarm could perform a joint strike on a target.¹⁴⁷ There are some who claim that swarms could be used in an offensive capacity for mass casualty and assassination purposes and might serve as a strategic deterrent, for example in lieu of chemical, biological and radiological weapons.¹⁴⁸

6.1.4 Saturating enemy air defences

Air defence is another area where swarm technology is expected to play a key role. In this context, swarms can be used to overwhelm and neutralize enemy air defence.¹⁴⁹ The European Union is currently funding a research project called Suppression Enemy Air Defense Swarm, which aims to develop a control algorithm that would reportedly “enable a mass of aerial drones to inspect the characteristics of air defense systems, distribute the information within the swarm and derive a plan of attack against weak points. Actions taken could include blinding radar sensors, overwhelming anti-aircraft fire with kamikaze-type tactics, or attacking sites with explosive or electronic-warfare payloads.”¹⁵⁰ The UK Secretary of State for Defence said on 11 February 2019 that the United Kingdom was to field swarming drones to confuse and overwhelm enemy air defences by the end of the year.¹⁵¹

¹⁴⁴ NavalDrones (2020).

¹⁴⁵ Long (2018).

¹⁴⁶ Liu (2019).

¹⁴⁷ STM (2019).

¹⁴⁸ Kallenborn & Bleek (2018, 523, 541). Using large swarms for attack or assassination purposes is also portrayed in fictional movies like the American action movie *Angel Has Fallen*, but also the civil society initiative *Slaughterbots*, presented during the meeting of the High Contracting Parties to the CCW in 2017.

¹⁴⁹ Lamothe (2016).

¹⁵⁰ Sprenger (2019).

¹⁵¹ Jennings & Cranny-Evans (2019).

6.1.5 Force protection

Swarms could also be used to protect high-end military platforms and troops during missions. They may be deployed, for example, around a convoy, ships or other assets to absorb enemy fire, or they could be used to move ahead of fighter jets, ships or ground troops to identify threats and, potentially, neutralize them.¹⁵² For example, the US Air Force's XQ-58A Valkyrie is designed to operate as a "loyal wingman", meaning it will fight alongside a human pilot – either as a single drone or as a swarm of drones – and absorb enemy fire.¹⁵³

6.1.6 Deception

Swarms could be used for deception operations to confuse the enemy. They could be used as decoys, perform false manoeuvres or deceive the adversary into thinking that the coordinated emissions from dispersed elements is a much larger vehicle moving through an area.¹⁵⁴ Similar decoy tactics have been deployed by Israeli forces in the Syrian Arab Republic, tricking Syrian radars into believing drones were attacking aircraft.¹⁵⁵

6.1.7 Dull, dirty and dangerous tasks

Swarms could also be used for dull, dirty and dangerous tasks. For example, they could be used for mine detection and cleaning. If one robot fails and a mine explodes, the other robots could continue their search.¹⁵⁶ Conversely, swarms could be used as mobile, self-replenishing mines. They could, for example, detect whether they are close to other mines and, if so, move to other areas. Such a capability is said to increase the disruptive capacity of mines.¹⁵⁷ In the field of maintenance, aerospace engine manufacturer Rolls-Royce is sponsoring projects examining the use of miniature robots that can perform visual inspections of engines.¹⁵⁸ This technology may be transferred to the military domain, potentially allowing for predictive inspection and maintenance of military vehicles. This will likely have implications for the operational readiness of the armed forces.

¹⁵² See, for example, the DARPA and Air Force Research Laboratory project Gremlins and the US Navy's swarm boats that can overwhelm adversaries. Smalley (2014); Wierzbanski (2019b).

¹⁵³ Liptak (2019).

¹⁵⁴ Scharre (2015). See, for example, what may have been a flock of birds causing a White House lockdown when it appeared on the radar as a small aircraft. Cohen et al. (2019).

¹⁵⁵ Kallenborn & Bleek (2018, 534).

¹⁵⁶ Navarro & Matía (2013).

¹⁵⁷ Defense Science Board (2016, 85).

¹⁵⁸ Rolls-Royce (2018).

6.1.8 Counter-swarms

Swarms may also be used to counter other swarms. The worldwide availability of small robotic platforms (particularly aerial vehicles such as hobby aircraft) raises widespread security concerns. Both sophisticated systems (e.g. large swarms operating under a centralized commander's intent but with decentralized execution)¹⁵⁹ as well as relatively crude systems (hundreds of commercially available drones carrying explosives or biological or chemical payloads) can be incredibly difficult to counter.¹⁶⁰ While swarms may be countered by other means, such as high-power microwave attacks or large shotguns with small munitions,¹⁶¹ countering swarms with swarms is an actively researched domain.¹⁶²

6.2 LIMITATIONS AND CHALLENGES

Even though swarm technology is being researched, developed and tested actively by many States, military swarms are not yet an operational reality. Significant challenges arise for militaries to make the leap from experimental testing to operational deployment. The next sections will discuss some of the chief limitations of existing swarms and the challenges related to operationalizing these technologies in a military environment.

6.2.1 Procedures for Test and Evaluation (T&E) and Verification and Validation (V&V)

Given the complexity and uncertainty that is typical for military environments, swarms would have to be able to assimilate, respond and adapt to dynamic situations that are not considered during their design.¹⁶³ To conduct the necessary operational T&E and V&V for large groups of robots (both hard- and software), there is a need for good laboratory infrastructure¹⁶⁴ as well as dynamic environments in which swarms can be tested under realistic conditions, taking into account possible adversary actions and the potential consequences of an unintended engagement or the loss of control of the system.¹⁶⁵

¹⁵⁹ Scharre (2014b, 38).

¹⁶⁰ National Academies of Sciences, Engineering, and Medicine (2018).

¹⁶¹ Interview with anonymous expert, 11 October 2019.

¹⁶² See, for example, the Naval Postgraduate School's experiments on counter-swarms in the context of the Advanced Robotic Systems Engineering Laboratory. Chung (2015).

¹⁶³ Ilachinski (2017, vi).

¹⁶⁴ Even creating controlled laboratories for testing can be challenging, as these require significant funding. To create a space to test ideas on hardware, Magnus Egerstedt, Professor at the Georgia Institute of Technology, created the Robotarium. In this 725-square-foot (67 square meters) laboratory, people can upload their programs and watch machines carry out their commands. Interview with anonymous expert, 18 October 2019.

¹⁶⁵ Group of Governmental Experts on Lethal Autonomous Weapons Systems (2019, 6); US Department of Defense (2017, 7).

6.2.2 Security challenges and vulnerabilities

In military operations, communication between units and between the human and the swarm are vulnerable to attack. Some commonly used communication methods in swarm R&D are wireless signalling over Bluetooth, Wi-Fi, radio, lidar, infrared or a mix of methods. These methods may work well in a controlled environment, but in a military environment, these forms of communication are vulnerable to jamming, spoofing, hacking, hijacking, manipulation or other electronic warfare attacks. Even without external influence in the form of malicious attacks, communication in a military context may not always be reliable (it can be interrupted and intermittent) or possible (e.g. underwater systems). Similar challenges apply to navigational techniques that are based on, for example, GPS or wireless beacons.¹⁶⁶ Promotional videos demonstrating swarm capabilities may thus look incredibly sophisticated – such as STM’s Kargu swarm performing a joint strike on a target – but many important questions regarding communication and navigation, as well as coordination and C2 models, remain unanswered.¹⁶⁷

6.2.3 Costs

Given the rapidly increasing cost of military hardware and personnel, affordability of new capabilities is an important factor in military R&D. It is often argued that individual robots of a swarm need not be expensive multimission systems but rather can be simple units, making them, potentially, dramatically cheaper than stand-alone weapon systems.¹⁶⁸ As a result, swarms of low-cost robots would be comparatively dispensable and, as such, could be used for high-risk missions where losing units does not prevent the swarm continuing the mission. While this may hold in theory, ongoing R&D demonstrates that the costs involved in developing and producing swarms can be relatively high. In particular in the context of targeting, swarms that can search for and identify targets, process the data, communicate with one another and navigate the battlefield all at the same time, can be quite expensive.¹⁶⁹ It may thus not be a given that a swarm of robots will, as a group, cost less than a single multimission robot.¹⁷⁰

¹⁶⁶ Beacons (as inspired by nature) can be placed in the area of operations and serve as a base station. A swarm of robots can spread out in the environment around the beacon and, after conducting the search, return to the beacon. This can be useful for, for example, search and rescue operations after a natural disaster. But using a beacon in a hostile environment will make it vulnerable to attack. Delft University of Technology (2019).

¹⁶⁷ STM (2019).

¹⁶⁸ Lachow (2017, 98); Scharre (2014b, 6).

¹⁶⁹ Safi (2019).

¹⁷⁰ Ilachinski (2017, 106).

6.2.4 Emergent behaviour

Emergent behaviour is group behaviour that arises from the interaction between the individual robots in the swarm. This behaviour is not programmed and cannot be readily explained from the behaviour at the individual robots' level.¹⁷¹ In the context of ongoing LAWS discussions, emergent behaviour typically has a negative connotation because it, allegedly, prevents decision makers from predicting a system's behaviour on the battlefield and, as such, increases unintended risks.¹⁷² In swarm robotics, however, emergent behaviour is said to be both a blessing and a curse.¹⁷³ On the one hand, emergent behaviour may be used to solve complex problems that cannot be solved by other means. On the other hand, emergent behaviour challenges prediction of the system's behaviour, potentially resulting in lack of trust and control by the user and a higher risk of undesired behaviour.

Whether emergent behaviours are inherently unpredictable or impossible to control remains a matter of debate. While some argue that emergent behaviour is inherently unpredictable,¹⁷⁴ others claim that prediction of certain simple behaviours is possible or that some elements of emergent behaviour may be universal, while recognizing that predicting detailed characteristics is more challenging.¹⁷⁵ As humans are relatively skilled at finding groups and patterns in everyday life, some experts argue that, in theory, humans may be uniquely suited to identify, categorize and alter swarm behaviour.¹⁷⁶ Also, some experts believe that control over swarms with emergent behaviour is possible – albeit complex – through design and modelling approaches.¹⁷⁷

How to adequately design appropriate machine-machine and human-machine interaction is an unanswered question that is complicated, in part, by the lack of a universal model that allows humans to understand complex emergent behaviour and take adequate responses in a timely manner. Without the ability to verify and trust the emergent behaviour of swarms in the situations in which they will be (or are intended to be) applied, it is likely that strict limits on their use in real-world, military environments will apply.¹⁷⁸ This uncertainty in predicting or even understanding swarm behaviour ex post seems to be one

¹⁷¹ Harvey (2018, 117).

¹⁷² For a detailed examination of unintentional risk in increasingly autonomous systems, see UNIDIR (2016); Scharre (2016).

¹⁷³ Harvey (2018).

¹⁷⁴ Some participants in United Nations CCW discussions on LAWS in 2016 argued that "autonomous 'swarms' would mean that such systems would be inherently unpredictable". Informal Meeting of Experts on Lethal Autonomous Weapons (2016, para. 40).

¹⁷⁵ Fromm (2005); Ilachinski (2017, 79). Walker et al. (2016, 1) further explain that "identifying the emergent behavior is often challenging, as deficiencies in the robot hardware or communication capabilities limit the amount of data that can be returned from the swarm. Furthermore, when there is significant noise or error in the robot data, the behaviors may not be readily apparent."

¹⁷⁶ Kolling et al. (2015, 15).

¹⁷⁷ Harvey (2018); interview with anonymous expert, 16 October 2019; interview with anonymous expert, 21 October 2019; interview with anonymous expert, 30 October 2019.

¹⁷⁸ Harvey (2018, 112).

reason that many developers express concern about the deployment of swarms in military contexts, in particular under the more advanced ensemble-level control and associated emergent coordination methods.

6.2.5 Adapting doctrine, concepts of operations and organizational frameworks

To allow for safe, responsible and lawful use of swarms, the technical possibilities offered by swarms will need to be supported by doctrinal, operational and organizational adjustments. As illustrated by the Perdix experiments, militaries may have to consider adapting their thinking.¹⁷⁹ This pertains to planning (of experiments and operations) but will, most likely, also require changes in military doctrine, concepts of operations and the organizational framework within which swarms are to be deployed. Some States, like the United States of America and the United Kingdom, have started exploring how to best implement these new technologies in their defence enterprises,¹⁸⁰ but further consideration of how military organizational structures and concepts should be adapted to allow for safe, responsible and lawful use of swarms (and how swarms may, in turn, affect these structures and concepts) is required.



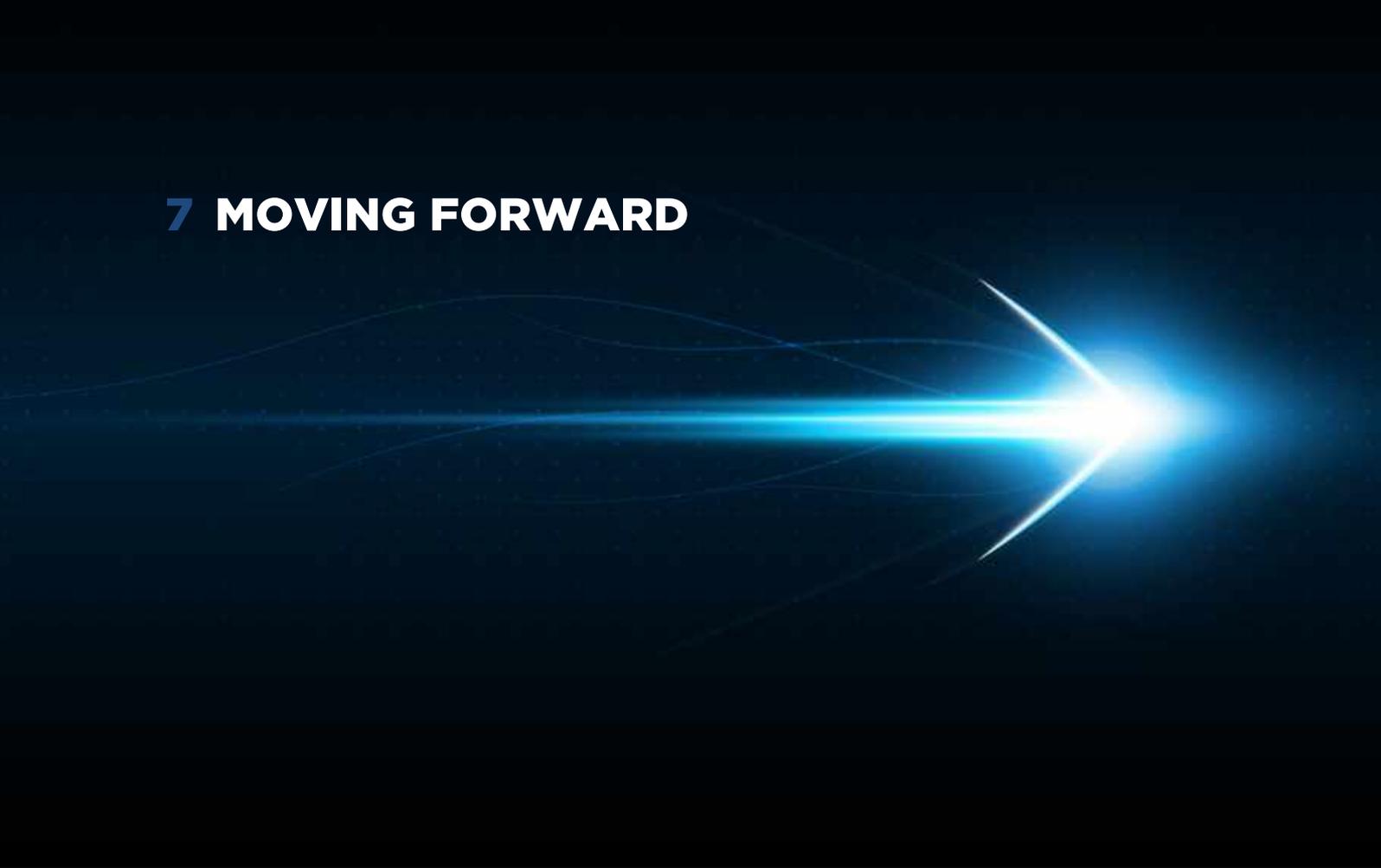
The winner of the Robotics Revolution will not be who develops this technology first or even who has the best technology, **but who figures out how to best use it.**

SOURCE: SCHARRE (2014A).

¹⁷⁹ When the US Air Force started testing its Perdix swarm (103 microdrones released from a canister in the back of military aircraft), a flight plan for each drone was requested. However, as these drones determine their own flight path in real time (adaptive formation flying), planners had to shift their thinking from “you need a flight plan” to “you need a box”. McCullough (2019).

¹⁸⁰ UK Ministry of Defence (2018); US Department of Defense (2017).

7 MOVING FORWARD



Whereas some argue that many of the issues that swarms raise could be addressed through improving the technology, operational concepts and training,¹⁸¹ others see particular value in multilateral discussions with the potential of creating new governance measures.¹⁸² Swarms have been discussed, albeit marginally, in the context of CCW LAWS discussions. In this context, efforts are primarily aimed at the control of LAWS, but many of the outcomes, such as the guiding principles, also have a bearing on swarms.

Although the 11 guiding principles have been developed in the context of LAWS discussions, the principles have a much wider application. For example, the principles confirm that international humanitarian law continues to apply fully to *all weapons systems* and, therefore, also applies to the development and use of LAWS and swarms. Another principle confirms that during the study, development, acquisition or adoption of *new weapons, means and methods of warfare*, States should comply with their obligations under international law. Any State that is developing swarms that may be considered new weapons, means or methods of warfare should, therefore, conduct a review process as early as possible (even as early as during the study of a new project).

Furthermore, principles confirming that accountability and responsibility must be ensured and cannot be transferred to machines apply, regardless of which

¹⁸¹ See, for example, Scharre (2014b, 35).

¹⁸² Article 36 (2019, 4); Homayounnejad (2018).

machines are used. And safeguards, risk assessments and mitigation measures “should be part of the design, development, testing and deployment cycle of emerging technologies *in any weapon systems*” [emphasis added].¹⁸³ The generality of these guiding principles and the fact that they typically confirm the application of existing obligations under international law were important factors leading to their adoption.

Ever since international discussions on LAWS started, States considered the “human element” as one of the main topics. But even though States agreed on the general idea of the need for some form of human involvement over weapons systems and the use of force, they could not agree on language that captured this objective until 2019, when they adopted the following principle:

“Human-machine interaction, which may take various forms and be implemented at various stages of the life cycle of a weapon, should ensure that the potential use of weapons systems based on emerging technologies in the area of lethal autonomous weapons systems is in compliance with applicable international law, in particular [international humanitarian law]. In determining the quality and extent of human-machine interaction, a range of factors should be considered including the operational context, and the characteristics and capabilities of the weapons system as a whole”.¹⁸⁴

However, the fact that States have reached formal consensus on these principles does not mean that they are well developed and commonly understood. Specifically, the quality and extent of human-machine interaction has been interpreted vastly differently among States, with some States calling for direct control over the weapon at all times and others arguing that human-machine interaction may be limited to the design and setting of operational parameters (and may not be necessary during the weapon’s operation). The interpretation of human-machine interaction may be even further complicated in the case of swarms for two reasons.

First, debates about human-machine interaction in the area of LAWS have focused primarily on the relationship between a human operator and a – or at least a limited number of – LAWS. When there is only a single vehicle or a limited number of vehicles, traditional forms of control are possible. However, for swarms of robotic units, it is necessary to rely on algorithms for formation, monitoring, spacing, flight path, task distribution, target identification and more.

This brings us to the **second** complicating factor: Besides human-machine interaction, swarms inevitably engage in machine-machine interaction. The

¹⁸³ For a full overview of all guiding principles, see Group of Governmental Experts on Lethal Autonomous Weapons Systems (2019, annex IV).

¹⁸⁴ Group of Governmental Experts on Lethal Autonomous Weapons Systems (2019, 3–4).

individual robots interact with other robots in the swarm to achieve a task and, in so doing, collective behaviour may arise. While this report shows there are different approaches to designing command, control architectures and cooperation methods that help mitigate some of the challenges that swarms raise, there seems to be no general method that explains the relationship between individual rules and (desired) group behaviour.¹⁸⁵

Some may argue that machine-machine behaviour in swarms inevitably means there is no human control. While this may be true in some circumstances, it is not an inevitable consequence of swarming technology. This report provided analysis of the various approaches to human control over swarms: (1) human-machine interaction by means of command, (2) a combination of human-machine and machine-machine interaction through the design and use of specific control architectures, and (3) machine-machine interaction resulting from the design and use of specific intra-swarm cooperation methods. In addition, this report put concepts of "human control" in the context of military decision-making, thereby introducing a framework of C2 within which concepts such as "human-machine interaction" and "meaningful human control" can be further discussed, analysed and developed.

Swarms will likely challenge the way in which humans exercise C2 in military decision-making. Therefore, the context provided in this report is highly relevant to discussions that aim to specify appropriate levels of human involvement in emerging technologies in the area of LAWS.

There is currently a dearth of studies investigating how humans can effectively command, control and coordinate swarms, and many open questions and issues for further study remain. These include, but are not limited to:

- What is an appropriate level of interaction between humans and swarms?
- How is the human-machine interaction influenced by the applied control architectures, coordination models, communication methods, mission type, and so on?
- What commands or orders might humans give to a swarm?
- What is emergent behaviour and can it be predicted or controlled in any way?
- How long and in which circumstances should humans trust a swarm to operate without the possibility of human intervention?
- How can the human infer the intent of the swarm, diagnose problems and assist a swarm?
- How can humans detect when a swarm has been hacked, jammed or spoofed?

¹⁸⁵ Ilachinski (2017, 123).

- How does one move from swarming in controlled environments (e.g. laboratories) to swarming in uncontrolled environments (e.g. battlefields)?

To harness the potential of swarm robotics and, ultimately, effectively and responsibly deploy swarms in military operations, these questions require significant further study. More research is needed, not only to increase our understanding of the technology itself but also to learn, test, evaluate and validate appropriate human-machine and machine-machine relationships.

As the international community continues discussions on LAWS in 2020 and 2021 and focuses on the further development and operationalization of the guiding principles, the role of human decision-making will undoubtedly be one of the core issues. While swarms are not yet operational and the technology is rather brittle, the prospect of military swarms is very real. By drawing on near-term technologies, such as swarms, and related C2 models in deliberations about the “human element”, the international community can move to develop a more comprehensive understanding of how control may or may not be exercised in military practice, now and in future operations.

BIBLIOGRAPHY

- 705th Training Squadron. 2017. *Joint Operation Planning Process for Air (JOPPA) Handbook*. Hurlburt Field: 705th Training Squadron.
- Agence France-Presse. 2015. 'US Military's New Swarm of Mini-Drones.' *DefenseNews*, 17 May. As of 11 December 2019: <http://www.defensenews.com/story/defense/international/americas/2015/05/17/cicadas-us-militarys-new-swarm-mini-drones/27494981>
- Alberts, David, & Richard Hayes. 2006. *Understanding Command and Control*. Washington, DC: DoD Command and Control Research Program.
- Aliman, Nadisha-Marie, & Leon Kester. 2019. "Requisite Variety in Ethical Utility Function for AI Value Alignment", paper, *International Joint Conference on Artificial Intelligence – AISafety Workshop*, Macao, 10–16 August 2019. As of 30 January 2020: http://ceur-ws.org/Vol-2419/paper_12.pdf
- Arquilla, John, & David Ronfeldt. 2000. *Swarming and the Future of Conflict*. Santa Monica: RAND Corporation.
- Article 36. 2013. 'Structuring Debate on Autonomous Weapon Systems.' As of 10 December 2019: www.article36.org/wp-content/uploads/2013/11/Autonomous-weapons-memo-for-CCW.pdf
- . 2014. 'Key Areas for Debate on Autonomous Weapon Systems.' As of 10 December 2019: www.article36.org/wp-content/uploads/2014/05/A36-CCW-May-2014.pdf
- . 2019. 'Swarms'. As of 17 February 2020: <http://www.article36.org/wp-content/uploads/2019/06/swarms.pdf>
- Bartles, Charles, & Lester Grau. 2018. *Russia's View of Mission Command of Battalion Tactical Groups in the Era of "Hybrid War"*. Fort Leavenworth: Foreign Military Studies Office. As of 13 December 2019: <https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/233611>
- Bashyal, Shishir, & Ganesh Venayagamoorthy. 2008. "Human Swarm Interaction for Radiation Source Search and Localization", paper, *2008 IEEE Swarm Intelligence Symposium*, St. Louis, 21–23 September 2008.
- Beal, Jacob. 2012. 'A Tactical Command Approach to Human Control of Vehicle Swarms.' In *Human Control of Bioinspired Swarms: Papers from the AAAI Symposium*. AAAI Technical Report FS-12-04. Menlo Park: AAAI Press.
- Boddens Hosang, Johannes. 2017. 'Rules of Engagement: Rules on the Use of Force as Linchpin for the International Law of Military Operations.' Dissertation. University of Amsterdam.
- Bonabeau, Eric, Guy Theraulaz & Marco Dorigo. 1999. *Swarm Intelligence: From Natural to Artificial Systems*. Oxford: Oxford University Press.
- Boulanin, Vincent, & Maaïke Verbruggen. 2017. *Mapping the Development of Autonomy in Weapons Systems*. Stockholm: Stockholm International Peace Research Institute.
- Campobasso, Michael. 2017. 'Leader-Follower Trajectory Generation and Tracking for Quadrotor Swarms.' Thesis. Embry-Riddle Aeronautical University.

- Cathcart, Blaise. 2012. 'Command and Control in Military Operations.' In *The Handbook of the International Law of Military Operations*, edited by Terry Gill & Dieter Fleck. Oxford: Oxford University Press.
- Chung, Timothy. 2015. 'ARSENAL: Advanced Robotic Systems Engineering Laboratory.' Naval Postgraduate School Wiki, 20 November. As of 10 December 2019: <https://wiki.nps.edu/display/~thchung/ARSENAL>
- Cohen, Zachary, Kristin Wilson, Noah Gray, Rene Marsh & Barbara Starr. 2019. "'Slow-Moving Blob' That May Have Been a Flock of Birds Caused White House Lockdown." CNN.com, 27 November, 00.45 a.m. GMT. As of 10 December 2019: <https://edition.cnn.com/2019/11/26/politics/white-house-lockdown-air-space/index.html>
- Cooney, Michael. 2015. 'Can Drones Hunt with Wolf Pack-Like Success? DARPA Thinks So.' Network World, 26 January, 11.29 a.m. PST. As of 10 December 2019 : <https://www.networkworld.com/article/2875573/can-drones-hunt-with-wolf-pack-like-success-darpa-thinks-so.html>
- Crandall, Jacob, et al. 2017. 'Human-Swarm Interaction as Shared Control: Achieving Flexible Fault-Tolerant Systems.' In *Engineering Psychology and Cognitive Ergonomics: Performance, Emotion and Situation Awareness*, edited by D. Harris. Cham: Springer.
- Crawford, Neta. 2013. *Accountability for Killing: Moral Responsibility for Collateral Damage in America's Post-9/11 Wars*. Oxford: Oxford University Press.
- Cruise, Robert, Erik Blasch, Sriraam Natarajan & Ali Raz. 2018. 'Cyber-Physical Command-Guided Swarm.' *DSIAC Journal* 5 (2): 23–30.
- Cummings, Mary. 2015. 'Operator Interaction with Centralized Versus Decentralized UAV Architectures.' In *Handbook of Unmanned Aerial Vehicles*, edited by K. Valavanis & G. Vachtsevanos, 977–92. Springer.
- Cummings, Mary, Jonathan P. How, Andrew Whitten & Olivier Toupet. 2011. 'The Impact of Human–Automation Collaboration in Decentralized Multiple Unmanned Vehicle Control.' *Proceedings of the IEEE* 100 (3): 660–71.
- Davis, Duane, Timothy Chung, Michael Clement & Michael Day. 2016. "Consensus-based data sharing for large-scale aerial swarm coordination in lossy communications environments", paper, *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems*, Daejeon, 9–14 October 2016.
- Defense Advanced Research Projects Agency (DARPA). 2019. 'OFFensive Swarm-Enabled Tactics (OFFSET).' As of 10 December: <https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics>
- Defense Science Board. 2012. *The Role of Autonomy in DoD Systems*. Task Force Report. Washington, DC: US Department of Defense. As of 13 December 2019: <https://fas.org/irp/agency/dod/dsb/autonomy.pdf>
- . 2016. *Summer Study on Autonomy*. Washington, DC: US Department of Defense. As of 27 December 2019: <https://www.hsdl.org/?view&did=794641>
- Delft University of Technology. 2019. 'Swarm of Tiny Drones Explores Unknown Environments.' Science Daily, 23 October. As of 10 December 2019: <https://www.sciencedaily.com/releases/2019/10/191023172112.htm>

- Department of Defence Science and Technology. 2019. 'Laser Detection and Ranging (LADAR).' Australian Government. As of 27 December: <https://www.dst.defence.gov.au/innovation/laser-detection-and-ranging-ladar>
- Distributed and Collaborative Intelligent Systems and Technology (DCIST). 2020. 'Home.' As of 13 January 2020: <https://www.dcist.org>
- Edwards, Sean. 2005. *Swarming and the Future of Warfare*. Santa Monica: RAND Corporation.
- Egerstedt, Magnus. 2011. 'Degrees of control.' *Nature* 473: 158–59. doi:10.1038/473158a
- Ekelhof, Merel. 2019a. 'The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targeting.' Dissertation. VU University Amsterdam.
- . 2019b. 'Moving Beyond Semantics on Autonomous Weapons: Meaningful Human Control in Operation.' *Global Policy* 10 (3): 343–48.
- Feng, Emily, & Charles Clover. 2017. 'Drone Swarms vs Conventional Arms: China's Military Debate.' *Financial Times*, 24 August. As of 10 December 2019: <https://www.ft.com/content/302fc14a-66ef-11e7-8526-7b38dcaef614>
- Flasinski, Mariusz. 2016. *Introduction to Artificial Intelligence*. Cham: Springer.
- Ford, Christopher. 2017. 'Autonomous Weapons and International Law.' *South Carolina Law Review* 63: 413–78.
- Fortinet. 2018. 'Fortinet Threat Landscape Report Reveals Attacks per Firm Increased by 82%.' Fortinet, 20 February. As of 10 December 2019: <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2018/threat-landscape-report-reveals-attacks-per-firm-increased.html>
- Fransman, Jeroen, & Leon Kester. 2012. *Utility Based Swarm Surveillance: A Nautical Case*. MP-SET-222-Fransman. Brussels: North Atlantic Treaty Organization Science and Technology Organization.
- Fromm, Jochen. 2005. 'Types and Forms of Emergence.' arXiv.org, 13 June. As of 10 December 2019: <https://arxiv.org/abs/nlin/0506028>
- Future of Life Institute. 2017. 'Slaughterbots.' YouTube, 13 November. As of 10 December 2019: https://www.youtube.com/watch?v=HipTO_7mUOw
- Giangreco, Leigh. 2018. 'DARPA Completes Second Phase of Swarming Demo.' FlightGlobal, 12 January. As of 10 December 2019: <https://www.flightglobal.com/news/articles/darpa-completes-second-phase-of-swarming-demo-444863>
- Global Guerrillas. 2012. 'Printing Drones by the Sheet (or How We Get to Tens of Billions of Drones by 2020).' Global Guerrillas, 16 February. As of 16 January 2020: <https://globalguerrillas.typepad.com/globalguerrillas/2012/02/printing-drones-by-the-sheet.html>
- Gorenburg, Dmitry. 2012. 'Challenges Facing the Russian Defense Establishment.' Russian Military Reform, 20 December. As of 13 December 2019: <https://russiamil.wordpress.com/tag/strategic-operational-commands>
- Group of Governmental Experts on Lethal Autonomous Weapons Systems. 2019. UN document CCW/GGE.1/2019/CRP.1/Rev.2, 21 August 2019.

- Hartnett, Kevin. 2018. "Smarticle" Robot Swarms Turn Random Behavior into Collective Intelligence.' *Quanta Magazine*, 18 February. As of 13 December 2019: <https://www.scientificamerican.com/article/ldquo-smarticle-rdquo-robot-swarms-turn-random-behavior-into-collective-intelligence>
- Harvey, John. 2018. 'The Blessing and Curse of Emergence in Swarm Intelligence Systems.' In *Foundations of Trusted Autonomy: Studies in Systems, Decision and Control*, edited by Abbass Hussein et al., 117–24. Cham: Springer.
- Homayounnejad, Maziar. 2018. *Autonomous Weapon Systems, Drone Swarming and the Explosive Remnants of War*. TLI Think! Paper 1/2018. London: King's College London.
- Ilachinski, Andrew. 2017. *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies*. Arlington: CNA.
- Informal Meeting of Experts on Lethal Autonomous Weapons Systems. 2016. UN document CCW/CONF.V/2, 16 June 2016.
- Integrated Defence Staff. 2017. *Joint Doctrine Indian Armed Forces*. New Delhi: Indian Armed Forces.
- Intel. 2018. 'Intel Breaks Guinness World Records Title and Lights Up the Sky at Winter Olympics with Intel Shooting Star Drones.' Intel.com/Newsroom, 9 February. As of 10 December 2019: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/02/Intel-Olympics-Drone-Fact-Sheet.pdf>
- Irvine, Caitlin. 2018. 'The Chinese Swarming Programme – Part Three of Three.' Security Distillery, 7 September. As of 13 December 2019: <https://thesecuritydistillery.org/all-articles/the-chinese-swarming-programme-part-three-of-three>
- Jasmine Swarm Robot Platform. 2019. 'Swarm Communication.' As of 13 December 2019: www.swarmrobot.org/Communication.html
- Jennings, Gareth, & Samuel Cranny-Evans. 2019. 'UK to Use "Swarming Drones" to Defeat Enemy Air Defences.' *Jane's Defence Weekly*, 11 February. As of 11 December 2019: <https://www.janes.com/article/86286/uk-to-use-swarming-drones-to-defeat-enemy-air-defences>
- Kallenborn, Zachary. 2018. 'The Era of the Drone Swarm is Coming, and We Need to Be Ready for It.' Modern War Institute, 25 October. As of 13 December 2019: <https://mwi.usma.edu/era-drone-swarm-coming-need-ready>
- Kallenborn, Zachary, & Philipp Bleek. 2018. 'Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons.' *The Nonproliferation Review* 25 (5–6): 523–43.
- Kania, Elsa. 2017. 'Swarms at War: Chinese Advances in Swarm Intelligence.' *China Brief* 17 (9). As of 13 December 2019: <https://jamestown.org/program/swarms-war-chinese-advances-swarm-intelligence>
- Kolling, Andreas, Steven Nunnally & Mike Lewis. 2012. "Towards Human Control of Robot Swarms", paper, *Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, Boston, 5–8 March 2012.
- Kolling, Andreas, Phillip Walker, Nilanjan Chakraborty, Katia Sycara & Michael Lewis. 2015. 'Human Interaction with Robot Swarms: A Survey.' *IEEE Transactions on Human-Machine Systems* 46 (1): 1–18.

- Kometer, Michael. 2007. *Command in Air War: Centralized versus Decentralized Control of Combat Airpower*. Alabama: Air University Press.
- Kordon, Arthur. 2010. *Applying Computational Intelligence*. Berlin: Springer.
- Lachow, Irving. 2017. 'The Upside and Downside of Swarming Drones.' *Bulletin of the Atomic Scientists* 73 (2): 96–101.
- Lamothe, Dan. 2016. 'Veil of Secrecy Lifted on Pentagon Office Planning "Avatar" Fighters and Drone Swarms.' *Washington Post*, 8 March. As of 11 December 2019: <https://www.washingtonpost.com/news/checkpoint/wp/2016/03/08/inside-the-secretive-pentagon-office-planning-skyborg-fighters-and-drone-swarms>
- Liptak, Andrew. 2019. 'The US Air Force's Jet-Powered Robotic Wingman Is Like Something out of a Video Game.' *The Verge*, 9 March, 1.00 p.m. EST. As of 14 January 2020: <https://www.theverge.com/2019/3/9/18255358/us-air-force-xq58-a-valkyrie-prototype-robotic-loyal-wingman-drone-successful-test-flight>
- Liu, Xuanzun. 2019. 'Chinese Helicopter Drones Capable of Intelligent Swarm Attacks.' *Global Times*, 9 May. As of 13 January 2020: <http://www.globaltimes.cn/content/1149168.shtml>
- Liu, Yang. 2017. 'Drone Swarming Technique May Change Combat Strategies: Expert.' *Global Times*, 13 February. As of 2 February 2020: www.globaltimes.cn/content/1032741.shtml
- Lomocano, Vincenzo, et al. 2018. 'Intelligent Drones Swarms for Search and Rescue Operations at Sea.' arXiv.org, 13 November. As of 11 December 2019: <https://arxiv.org/abs/1811.05291>
- Long, Drake. 2018. 'China Releases Video of 56-Boat Drone Swarm near Hong Kong.' *The Defense Post*, 2 June. As of 14 January 2020: <https://thedefensepost.com/2018/06/02/china-56-boat-drone-swarm-hong-kong>
- Marr, Bernard. 2017. 'The 4Ds of Robotization: Dull, Dirty, Dangerous and Dear.' *Forbes*, 16 October. As of 27 December 2019: <https://www.forbes.com/sites/bernardmarr/2017/10/16/the-4-ds-of-robotization-dull-dirty-dangerous-and-dear>
- McCann, Carol, & Ross Pigeau. 2002. *The Human in Command: Exploring the Modern Military Experience*. New York: Springer.
- McCullough, Amy. 2019. 'The Looming Swarm.' *Air Force Magazine*, 22 March. As of 13 December: <http://www.airforcemag.com/MagazineArchive/Pages/2019/April%202019/The-Looming-Swarm.aspx>
- McLurkin, James, et al. 2006. "Speaking Swarmish: Human-Robot Interface Design for Large Swarms of Autonomous Mobile Robots", paper, *AAAI Spring Symposium*, Stanford, 27–29 March 2006.
- McMullan, Thomas. 2019. 'How Swarming Drones Will Change Warfare.' *BBC News*, 16 March. As of 23 December 2019: <https://www.bbc.com/news/technology-47555588>

- Ministry of Defence of the Netherlands. n.d. *Command and Control*. Joint Doctrine Publication 5. The Hague: Ministry of Defence. As of 6 February 2020: <https://english.defensie.nl/binaries/defence/documents/publications/2012/03/13/joint-doctrine-publication-5-command-and-control-en/Joint+Doctrine+Publication+5+Command+and+Control+EN.pdf>
- National Academies of Sciences, Engineering, and Medicine. 2018. Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations: Abbreviated Version of a Restricted Report. Washington DC: National Academies Press.
- NavalDrones. 2020. 'CARACaS (Control Architecture for Robotic Agent Command and Sensing).' As of 10 January: <http://www.navaldrones.com/CARACAS.html>
- Navarro, Iñaki, & Fernando Matía. 2013. 'An Introduction to Swarm Robotics.' *International Scholarly Research Notices* 2013: 608164. doi:10.5402/2013/608164
- Noorman, Merel. 2014. 'Responsibility Practices and Unmanned Military Technologies.' *Science and Engineering Ethics* 20, 809–26.
- North Atlantic Treaty Organization (NATO). 2004. *Air Interdiction and Close Air Support*. AJP-3.3.2. Brussels: NATO.
- . 2016a. *Allied Joint Doctrine for Air and Space Operations*. AJP-3.3(B). Brussels: NATO Standardization Office.
- . 2016b. *Allied Joint Doctrine for Joint Targeting*. AJP-3.9(A). Brussels: NATO Standardization Office.
- . 2017. *Allied Joint Doctrine*. AJP-01(E). Brussels: NATO Standardization Office.
- North Atlantic Treaty Organization (NATO), European Union (EU) & United Nations. 2015. Informal Interorganizational Military Glossary of Abbreviations, Terms and Definitions Related to Conflict Prevention (CP) and Defence and Related Security Capacity Building (DCB).
- Pandit, Rajat. 2019. 'India, US to Collaborate on Drone Swarms and Other Military Hi-Techs.' *Times of India*, 24 October. As of 27 December 2019: <https://timesofindia.indiatimes.com/india/india-us-to-collaborate-on-drone-swarms-other-military-hi-techs/articleshow/71747116.cms>
- Perry, Caroline. 2014. 'The 1,000-Robot Swarm.' *Harvard Gazette*, 14 August. As of 13 December 2019: <https://news.harvard.edu/gazette/story/2014/08/the-1000-robot-swarm>
- Raz, Ali, et al. 2019. "Enabling Autonomy in Command and Control via Game-Theoretic Models and Machine Learning with a Systems Perspective", paper, *AIAA SciTech Forum*, San Diego, 7–11 January 2019.
- Roborder. 2019. 'Aims and Objectives.' As of 13 December: <https://roborder.eu/the-project/aims-objectives>
- Rolls-Royce. 2018. 'Rolls-Royce Demonstrate the Future of Engine Maintenance with Robots Can Crawl inside Engines.' [Rolls-Royce.com/Press Releases](https://www.rolls-royce.com/PressReleases), 17 July. As of 11 December 2019: <https://www.rolls-royce.com/media/press-releases/2018/17-07-2018-rr-demonstrates-the-future-%20of-engine-maintenance-with-robots.aspx>
- Safi, Michael. 2019. 'Are Drone Swarms the Future of Aerial Warfare?' *Guardian*, 4 December. As of 11 December 2019: <https://www.theguardian.com/news/2019/dec/04/are-drone-swarms-the-future-of-aerial-warfare>

- Scharre, Paul. 2014a. *Robotics on the Battlefield – Part I: Range, Persistence and Daring*. Washington, DC: Center for a New American Security.
- . 2014b. *Robotics on the Battlefield – Part II: The Coming Swarm*. Washington, DC: Center for a New American Security.
- . 2015. 'Unleash the Swarm: The Future of Warfare.' *War on the Rocks*, 4 March. As of 13 December 2019: <https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare>
- . 2016. *Autonomous Weapons and Operational Risk*. Washington, DC: Center for a New American Security.
- . 2018. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company.
- Schulzke, Marcus. 2013. 'Autonomous Weapons and Distributed Responsibility.' *Philosophy and Technology* 26: 209–13.
- Smalley, David. 2014. 'The Future Is Now: Navy's Autonomous Swarmboats Can Overwhelm Adversaries.' Office of Naval Research, 5 October. As of 11 December 2019: <http://www.onr.navy.mil/Media-Center/Press-Releases/2014/autonomous-swarm-boat-unmanned-caracas.aspx>
- South China Morning Post. 2017. 'China Drone Show: More Than 1,000 Drones Put On Light Show in China.' YouTube, 11 December. As of 6 February 2020: www.youtube.com/watch?v=5QP6InPZaIY
- Sprenger, Sebastian. 2019. 'Europeans Propose Sicking Self-Learning Drone Swarms on Air Defences.' *DefenseNews*, 22 October. As of 11 December 2019: <https://www.defensenews.com/global/europe/2019/10/22/europeans-propose-sicking-self-learning-drone-swarms-on-air-defenses>
- STM. 2019. 'Kargu – The Kamikaze Drones Getting Ready for the Swarm Operation.' YouTube, 17 July. As of 13 December 2019: <https://www.youtube.com/watch?v=3d28APIfwSI>
- Stratcore Group. 2020. 'Communication Systems.' *New Warfare*. As of 9 January: http://newwarfare.com/index.php?task=main_story&&id=142
- Sugiura, Yasuyuki. 2017. 'The Joint Operation Structure of the Chinese People's Liberation Army with Focus on the Reorganization of the Chain of Command and Control under the Xi Jinping Administration.' *NIDS Journal of Defense and Security* 18: 3–31.
- UK Ministry of Defence. 2017. *Future of Command and Control*. Joint Concept Note 2/17. Swindon: Development, Concepts and Doctrine Centre.
- . 2018. *Human-Machine Teaming*. Joint Concept Note 1/18. Swindon: Development, Concepts and Doctrine Centre.
- United Nations Department of Peacekeeping Operations (UNDPO). 2016. *Standard Operating Procedure on Force and Sector Commander's Evaluation of Subordinate Military Entities in Peacekeeping Operations*. As of 27 December 2019: <http://dag.un.org/handle/11176/387393>
- United Nations Development Programme (UNDP). 2018. *Standard Operating Procedure for Immediate Crisis Response*. New York: UNDP.

- United Nations Institute for Disarmament Research (UNIDIR). 2014. *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward*. Geneva: UNIDIR. As of 11 December 2019: <https://www.unidir.org/publication/weaponization-increasingly-autonomous-technologies-considering-how-meaningful-human>
- . 2016. *Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies*. Geneva: UNIDIR. As of 11 December 2019: <http://www.unidir.org/files/publications/pdfs/safety-unintentional-risk-and-accidents-en-668.pdf>
- US Air Force. 2016. *Annex 3-0 - Operations and Planning*. Maxwell: LeMay Center for Doctrine. As of 6 February 2020: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-Annex-OPERATIONS-PLANNING.pdf
- . 2019. *Annex 3-60 - Targeting*. Maxwell: LeMay Center for Doctrine. As of 6 February 2020: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-60/3-60-Annex-TARGETING.pdf
- US Department of Defense. 2017. 'Autonomy in Weapon Systems.' Directive 3000.09. As of 13 February 2020: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf>
- US Department of the Army. 2003. 'Command and Control.' In *Mission Command: Command and Control of Army Forces*. Field Manual No. 6-0. Washington, DC: Department of the Army. As of 10 December 2019: <https://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm>
- . 2011. *Army Tactical Standard Operating Procedures*. Washington, DC: Department of the Army. As of 27 December 2019: <https://www.globalsecurity.org/military//library/policy/army/atp/atp3-90-90.pdf>
- US Joint Chiefs of Staff. 2010. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication 1-02. As of 6 February 2020: https://usacac.army.mil/sites/default/files/misc/doctrine/CDG/cdg_resources/manuals/jps/jp1_02.pdf
- . 2014. *Close Air Support*. Joint Publication 3-09.3. As of 6 February 2020: https://www.public.navy.mil/fltfor/ewtgant/Documents/courses/cin/TACP%20Docs%20K-2G-3615/jp3_09_3%20Jul2015.pdf
- . 2019. *Joint Fire Support*. Joint Publication 3-09. As of 13 December 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf
- Walker, Phillip, et al. 2016. "Characterizing Human Perception of Emergent Swarm Behaviors", paper, *IEEE International Conference on Systems, Man, and Cybernetics*, Budapest, 9–12 October.
- Wierzbanski, Scott. 2019a. 'Collaborative Operations in Denied Environment (CODE).' Defense Advanced Research Projects Agency. As of 10 December: <https://www.darpa.mil/program/collaborative-operations-in-denied-environment>
- . 2019b. 'Gremlins.' Defense Advanced Research Projects Agency. As of 10 December: <https://www.darpa.mil/program/gremlins>

Woo, Marcus. 2014. 'Scientists Program Largest Swarm of Robots Ever.' *Wired*, 14 August. As of 13 December 2019: www.wired.com/2014/08/largest-robot-swarm-ever

Xu, Dongdong, et al. 2014. 'Behavior-Based Formation Control of Swarm Robotics.' *Mathematical Problems in Engineering* 2014: 205759. doi:10.1155/2014/205759

ANNEX

LIST OF CONSULTED EXPERTS	
NAME	AFFILIATION
Dr. Timothy H. Chung	Tactical Technology Office, Defense Advanced Research Projects Agency
Prof. Mary "Missy" Cummings	Professor at the Department of Electrical and Computer Engineering at Duke University
Prof. Raffaello D'Andrea	Professor of Dynamic Systems and Control, ETH Zürich
Dr. Guido De Croon	Associate Professor, Micro Air Vehicle Laboratory, Section Control and Simulation of the Department Control and Operations, Faculty of Aerospace Engineering at Delft University of Technology
Dr. Magnus Egerstedt	Steve W. Chaddick School Chair and Professor, School of Electrical and Computer Engineering at Georgia Institute of Technology
Dr. Joost Ellerbroek	Assistant Professor, Section Control and Simulation of the Department Control and Operations, Faculty of Aerospace Engineering at Delft University of Technology
LTC Martijn Hädicke	Program officer Robotics and Autonomous Systems, Netherlands Army
Dr. Martin Hagström	Deputy Research Director, Swedish Defence Research Agency
David Hambling	Freelance journalist on science and technology and author of Swarm Troopers
Dr. Andy Ilachinski	Principal Research Scientist, CNA's Center for Naval Analyses
Dr. Leon Kester	Senior Research Scientist, TNO Defence, Safety, and Security
COL Christopher Korpela	Associate Professor and Director of the Robotics Research Center, United States Military Academy at West Point

Jean-Charles Ledé	United States Air Force Research Laboratory
Dr. John Matsumura	Senior engineer, the RAND Corporation
Prof. Alcherio Martinoli	The Distributed Intelligent Systems and Algorithms Laboratory at L'Ecole Polytechnique Fédérale de Lausanne
Dr. Alyssa Pierson	Research Scientist, Massachusetts Institute of Technology
Dr. Ali K. Raz	Visiting Assistant Professor, School of Aeronautics and Astronautics at Purdue University
Dr. Jean-Marc Rickli	Head, Global Risks and Resilience at the Geneva Centre for Security Policy
Dr. Ludovic Righetti	Associate Professor, the Tandon School of Engineering of New York University
Paul Scharre	Senior Fellow and Director of the Technology and National Security Program, the Center for a New American Security
Prof. Katia Sycara	Research Professor, Robotics Institute at Carnegie Mellon University
Maaïke Verbruggen	Doctoral Researcher, Institute for European Studies at Vrije Universiteit Brussel
Dr. Sean Wilson	Research Engineer and Director of the Robotarium Laboratory, Georgia Institute of Technology
Kelvin Wong	Unmanned Systems Editor at Jane's International Defence Review, editor at Jane's Unmanned Maritime Vehicles, Jane's Group UK
+ 5 Experts Who Wish To Remain Anonymous	



@UNIDIR

WWW.UNIDIR.ORG

40 | **UNIDIR** UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH