02

Age of Autonomous Weapons Systems

SUMMER 2021

GOOD DATA INITIATIVE

Good Data Initiative

The Good Data Initiative (GDI) is an independent, student-run think tank for intergenerational and interdisciplinary debate on the data economy. We conduct research around some of the most pressing issues resulting from the data and artificial intelligence revolution, as well as advise & host events on the impact of the data economy on humans, organisations, and society.

GDI was founded in early 2020 by students at the University of Cambridge. We rapidly evolved in response to the struggles we saw bright, motivated students going through as they searched for meaningful opportunities during the COVID-19 pandemic. As internships were cancelled, job markets tightened, and organisations shifted to remote work, we realised there were limited alternatives for ambitious & curious young minds to gain meaningful early professional experience, much less upskill themselves as thought leaders & change makers shaping the future of the data economy.

GDI analysts engage in high-quality, nonpartisan research such as this GDI Review to inform industry leaders and policy makers about issues we believe are of crucial importance in the near future. Research for these GDI Reviews is conducted alongside our members' University studies and/or work for the purpose of developing & sharing the resulting expertise. We strive for completeness and accuracy in our work; any omissions or errors — human or machine — are unintended and seen as opportunities to learn.

Further information about GDI and copies of GDI's published reports can be found at **www.gooddatainitiative.com**. Comments and/or inquiries are welcome at **hi@gooddatainitiative.com**.

© 2021 Good Data Initiative

02

AGE OF AUTONOMOUS WEAPONS SYSTEMS

AUGUST 2021

HANNA CORSINI, MA
LINNEA TYBÄCK

GDI **REVIEW**

TABLE OF CONTENTS

Cover image: © Baykar via CC BY-SA 4.0

EXECUTIVE **SUMMARY**

AGE OF AUTONOMOUS WEAPONS SYSTEMS

We are at the dawn of the Age of Autonomous Systems. This revolution is driven by the fast-paced development of cutting-edge technologies in the civilian sector, with advancements in Artificial Intelligence and Big Data acting as disrupting forces in contemporary and future warfare.

Understanding the consequences of such evolution is important not only for armed forces, but also for those companies leading this technological progress in fields such as machine learning, facial recognition, and robotics. We at GDI believe that calling attention and awareness to this is crucial. Previous discussions on autonomous weapons systems (AWS) have primarily focused on either the moral, ethical, and legal obligations of this new type of warfare or specific technical details, rather than approaching it from systems-based perspective as done here. This resulting report is designed to better inform technology companies and start-ups in the IT, AI, and robotics sectors of foreseeable challenges associated with this field.

Based on our identification of the unique set of challenges that we believe the Age of Autonomous Systems poses to civilian-military cooperation, we have elaborated three key action areas for involved stakeholders:

1. IMPROVE STAKEHOLDER TRUST AND COMMUNCIATION CULTURE

BUILD TRUST IN LONG-TERM PPPs: Communication is the first step in creating an atmosphere of trust between stakeholders involved in the development of robotic and autonomous systems (RAS) for military use. This can also be achieved by building long-term private-public partnerships (PPPs) throughout the phases of the autonomous system life cycle. Trust is vital to this process since developers are required to modify and advance these systems (given that AI systems are never 'finished,' but rather demand updates tailored by data-based feedback received during their deployment). Contracts should clearly state the tasks and responsibilities of all stakeholders during each phase of development and training, and integrate under which terms a partnership can be terminated.

PRIORITIZING COMMUNICATION CULTURE: Given the variety of stakeholders involved in the life cycle of autonomous systems, creating a strong, clear communication culture is important. This action can help stakeholders to vocalize concerns, identify challenges, evaluate solutions, and overcome additional possible tensions caused by different organizational and managerial cultures.

2. ESTABLISH CLEAR BOUNDARIES AND ACCOUNTABILITY

APPROPRIATELY TRAIN MILITARY PERSONAL: It is developers' duty to ensure that end-users have confidence and an understanding of the technology's limitations when interacting with the autonomous system. As current international humanitarian law places the responsibility and accountability for these systems in deployment in the hands of the military (which may be modified, if stated otherwise in a future international legal framework), it is essential that commanders and operators have sufficient technical knowledge of these systems before deploying them in the battlefield, beyond their standard operational training.

ESTABLISH CODES OF CONDUCT: The main purpose of establishing codes of conduct is to provide clear manuals directly linking technological requirements to military objectives. These might include, for instance, the responsibilities of involved parties; improvements and potential operational shortcomings; issues with datasets (e.g., quality, real-life similarity); and the re-use and re-selling of technologies by a company to other countries or actors after the end of the contract. These codes will also establish clearly that system ownership lies with military (i.e., as an institution of the state).

DELINEATE PPP BOUNDARIES PRIOR TO COLLABORATION: As technological innovation is being primarily driven by civilian companies, the RAS and AWS revolution is characterized by the development of dual-use technologies. For civilian IT firms, this means that their products (both hardware and software) may be used without their knowledge for non-civilian purposes. Being aware and informed of this – as well as clearly identifying possible ethical concerns – before entering a cooperation with the military is vital for cohesion within the company itself. If a civilian company opts to enter such a collaboration, it is critical that they establish clear PPP boundaries for that specific enterprise.

BALANCE TRADE-OFFs OF MILITARY FUNDING: Smaller technology companies with no prior military ties will face a trade-off between accepting military funding versus rejecting it (such as for ethical reasons). In considering whether to accept military funding, it is crucial for the leadership of such companies to equally consider both potential economic and social consequences, including but not limited to: loss in revenue from public boycotts; restrictions connected to military funding; internal opposition from company employees; the personal moral and ethical convictions of the firm's leadership; and whether accepting this funding is in alignment with the purpose of the firm.

3. PROACTIVE MANAGEMENT OF DATA, DATA ANALYSIS, & FURTHER TECHNOLOGICAL DEVELOPMENT

MILITARY-BASED MANAGEMENT AND ANALYSIS OF BIG DATA: The military has collected a significant volume of raw data through previous missions and other related activities which cannot be used in its current state, given it is unstructured and stored across unintegrated databases. The authors suggest that civilian companies provide IT-solutions alongside their project deliverables that allow the military-based automated analyses of these datasets, which can be used to effectively train algorithms used in autonomous systems.

Provide IT-solutions for 'meaningful human control': In the current climate of uncertainty around international legal frameworks regarding armed forces' used of autonomous systems, private companies can still offer IT-based solutions that introduce greater human control over these machines. We envision these solutions including but not limited to: building in time frames allowing a human to veto the selected target before the machine attacks it; requiring human approval before the machine can proceed with a lethal strike; in the list of targets provided by the machine, visually depicting human targets to be attacked as humans; etc.

For any civilian technology company, deciding to engage with robotic and autonomous weapons systems' development (and ensuing technical support) requires careful consideration and, for leadership, the assumption of responsibility for this choice. Based on our research, we believe that constructive, open dialogue and proactive awareness of foreseeable challenges in this field will allow key stakeholders to make better informed decisions regarding which path(s) of engagement they choose to follow, as well as increase transparency around the likely organizational and societal consequences of these actions.

AGE OF AUTONOMOUS WEAPONS SYSTEMS
GLOSSARY

CCW	United Nations Convention on Certain Conventional Weapons
DARPA	Defense Advanced Research Projects
IHL	International Humanitarian Law
LAWS	Lethal Autonomous Weapon Systems
MLP	Machine Learning Processes
PPP	Public-Private Partnership
RAS	Robotic and Autonomous Systems
UAV	Unmanned Aerial Vehicles

AGE OF AUTONOMOUS WEAPONS SYSTEMS
PREFACE & ACKNOWLEDGEMENTS

Earlier this year, UN Secretary General Antonio Guterres called for governments around the world to focus on ten urgent priorities for 2021. While the first of these – responding to the ongoing COVID-19 pandemic – still remains a task at hand, the authors of this GDI Review noted two additional priorities that have invigorated our work on this project. These included a call to "reverse the erosion of the nuclear disarmament and non-proliferation regime," as well as to, "seize the opportunities of digital technologies while protecting against their growing dangers." We believe that both of these align with the need for greater understanding and informed stakeholder stewardship of the development of Lethal Autonomous Weapons Systems (LAWS).

Through this GDI Review, we have aimed to contribute a high-level, technology-focused systems perspective to a topic often presented only through opaque, deeply technical work or via highly polarized moral and ethical lenses. We believe that centering on the development and deployment of the LAWS technology itself – including the unusual double-loop method of developing and training LAWS and related robotic and autonomous systems – can help key actors to clarify their thinking on future public-private partnerships as well as more transparently locate accountability as they move forward.

Among the various conversations we had that informed the development of this work, we would like to thank the core GDI Research Team for their feedback throughout the development of this GDI Review (and especially following an early presentation of it in February 2021). We hope that this work serves to support fruitful and constructive future dialogue on LAWS, shedding additional light and providing a nuanced and critical analysis of this issue.

AGE OF AUTONOMOUS WEAPONS SYSTEMS
INTRODUCTION

Neither collaboration between armed forces and the private sector nor the use of cutting-edge technologies for military purposes are new phenomena. However, fast-paced developments in the field of Artificial Intelligence (AI) from the private sector are being increasingly coupled with available big data to produce something new: the dawn of a new era of warfare.

Some experts have highlighted the positive sides of this revolution, with its potential to minimize casualties during war; allow operations to proceed with greater ease in hostile environments; sustain missions over longer periods than humans can physically endure; and enable machines to make decisions at increasingly high speeds that outpace human capabilities.[1] Others depict a more negative picture, arguing that these technologies may reduce the financial cost, duration, violence, and casualties necessary to achieve a State's strategic goals, thus lowering barriers to entering an armed conflict.

The ability to purchase these new technologies (both software and hardware) from the internet and other commercial sources also raises the risk of proliferation and the ability of non-state armed groups to obtain and use them.[2] Experts and researchers within the AI/robotic communities have further warned against 'killer robots' – unstoppable machines designed to kill – leading to a technological 'point of no return' and the possible destruction of mankind.[3]

These views all have in common a belief that these technological developments have the potential to fundamentally revolutionize the future of warfare. What has changed in the past few years? What are the challenges and questions stakeholders need to be addressing today? What do these changes mean for partnerships between the civilian and the military sectors? And finally, what should the stakeholders within this ecosystem – especially civilian companies developing the technologies used for this new type of warfare – be aware of?

Rather than presenting either deeply technical, specialist considerations or dwelling on catastrophic and apocalyptic possible futures, this GDI report instead aims to bring a new voice to this conversation. In this report, we approach the creation and deployment of Lethal Autonomous Weapons Systems (LAWS) and Robotic and Autonomous Systems (RAWS) through a systems-based perspective. This enables us to clearly identify key stakeholders, clarify the overall ecosystem, and present several practical recommendations for how stakeholders – and civilian technology companies in particular – can better proceed in deciding how and if they choose to engage in this space.

[1] *Ben Koppelman, 'How Would Future Autonomous Weapon Systems Challenge Current Governance Norms?' (2019) 164 RUSI Journal 98.*

[2] *Michael W Meier, 'Emerging Technologies and the Principle of Distinction' in Ronald TP Alcala and Eric Talbot Jensen (eds), The Impact of Emerging Technologies on the Law of Armed Conflict (Oxford University Press 2019).*

[3] *Michael W Meier, 'Lethal Autonomous Weapons Systems' in Christopher M Ford and Winston S Williams (eds), Complex Battlespaces (Oxford University Press 2019).*

THE LANDSCAPE OF AWS

SECTION 1: ROBOTIC AND AUTONOMOUS SYSTEMS IN THE MILITARY SECTOR REVOLUTION

INTRODUCTION

We are entering a new era of warfare[4]: The Age of Autonomous Systems[5]. In a similar vein, some authors argue that we are about to witness the next revolution of military affairs following gunpowder and nuclear weapons[6].

A recent example of this is the Nagorno-Karabakh conflict between Armenia and Azerbaijan, started in late September 2020 and concluded after 44 days: Unmanned Aerial Vehicles (commonly called drones) were massively deployed by Azerbaijani forces, dominating the skies and enabling the Azerbaijani forces to achieve a decisive strategic advantage. These UAVs were operationally integrated with fire from manned aircraft and land-based artillery, though also frequently used their own ordinance to destroy various high-value military assets. For instance, the Turkish-made Bayraktar TB2 demonstrated the versatility of UAV platforms, performing well in targeting and destroying enemy defenses both by providing (a) identification and targeting data and (b) by carrying smart, micro guided munitions to kill targets on their own.[7]
At the heart of this revolution is a debate over autonomy, given its core of whether machine decision-making should replace human decision-making in modern warfare[8]. It is in this context that we encounter the term "Lethal Autonomous Weapon Systems" (LAWS) – a phrase admittedly less emphatic than that of 'killer robots'. LAWS became an international issue in April 2013, when the annual report of the UN Human Rights Council by Christof Heyns, the Special Rapporteur on extrajudicial, summary, or arbitrary executions, highlighted that these weapons raise two main concerns: first, their compliance with International Humanitarian Law (IHL); and second, ethical considerations, namely delegating to a robot the power of life and death over a human being. Furthermore, in 2013, the high contracting parties to the Convention on Certain Conventional Weapons (CCW) decided to hold informal discussions on LAWS yearly. In 2016, they also established a Group of Governmental Experts (GGE), with the mandate to assess questions related to emerging technologies in the area of LAWS.[9]

Even though LAWS-related issues are consistently present even in official debates within the UN, there remains no consensus as to their definition. The most used definition comes from the International Committee of the Red Cross, which defines LAWS as: "...any weapon system with autonomy in its critical functions. That is, a weapon system that can select (i.e. search for or detect, identify, track, select) and attack (i.e. use force against, neutralize, damage or destroy) targets without human intervention".[10] What appears to be consensual across definitions, though, is that autonomy includes functions deemed to be critical, encompassing the acquisition of a target and the decision to kill.[11]

Others prefer to differentiate between LAWS and Robotic and Autonomous Systems (RAS). The latter is an accepted term in academia and within the science and technology community highlighting both the physical (robotic) and cognitive (autonomous) aspects of these systems. Hence, RAS are defined as systems with a robotic element, an autonomous element, or, more commonly, both.[12] In this report we will use RAS by default, as it is an all-encompassing term referring to systems with any degree of autonomy and any military designation – hence, the definition includes, but is not limited to, AWS.[13] More specific ethical and legal issues raised by using AWS, especially in their lethal, offensive functions, will also be discussed later in this report.

[4] As it is presented in the work by Martin Van Creveld, Technology and War: From 2000 BC to the Present (The Free Press and Collier Macmillan Publishers 1989), one can divide the military history into four eras: "Age of Tools" (until 1500 AD, technology driven by muscles of humans or animals); "Age of the Machine" (greater professional skills and substitution of firepower mass rather than manpower mass); "Age of Systems" (emphasis on integration of technology into complex networks); "Age of Automation" (use of automated systems, requiring human input during at least one stage of deployment).

[5] Maxim Worcester, 'Autonomous Warfare – A Revolution in Military Affairs', vol 49 (2015).

[6] Meier (2019).

[7] Shaan Shaikh and Wes Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic & International Studies, 8 December 2020. Available: https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense

[8] Koppelman (2019)

[9] L Righetti and others, 'Lethal Autonomous Weapon Systems [Ethical, Legal, and Societal Issues]' (2018) 25 IEEE Robotics and Automation Magazine 123.

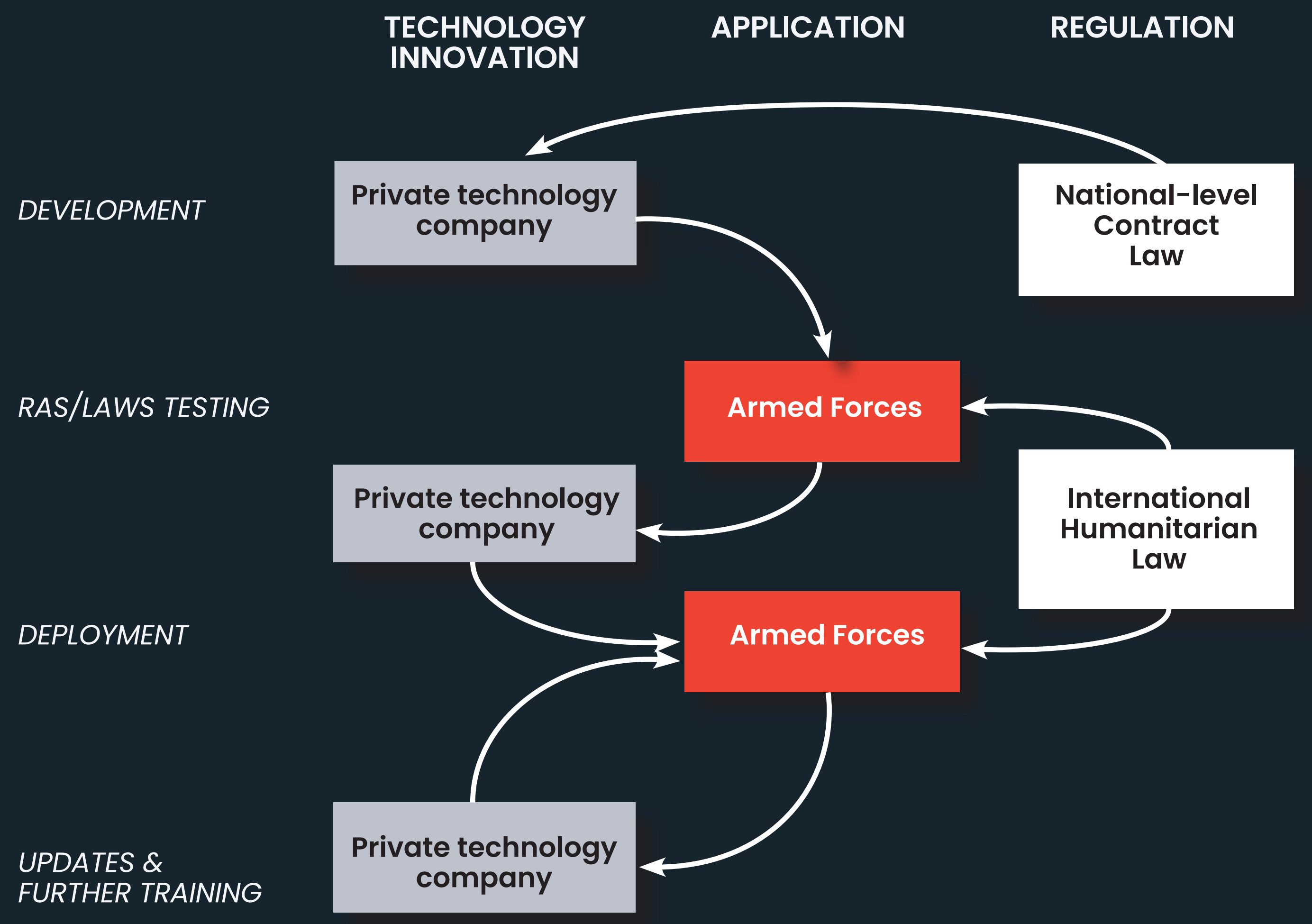
[10] Expert Meeting, 'Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons'.

[11] Righetti and others (2019).

[12] Esther Chavannes and Amit Arkhipov-Goyal, 'Towards Responsible Autonomy The Ethics of RAS in a Military Context' (2019).

[13] Most applications of RAS in a military setting do not fulfil lethal functions and also span a variety of roles (such as surveillance, logistics, medical support, maintenance, communication and engineering). This can be shown through a few figures: it is estimated that out of the known 500 RAS in operation today worldwide, 30% are designated for the use of force, within which 55% are used for defensive and 45% for offensive purposes. In sum, only 14% of all deployed RAS fulfil lethal offensive functions. It should be noted that such figures are

FIGURE 1: HIGH-LEVEL PROCESS MAP OF STAKEHOLDER INVOLVEMENT IN THE DEVELOPMENT AND DEPLOYMENT OF AUTONOMOUS WEAPONS SYSTEMS


TECHNOLOGY INNOVATION
APPLICATION
REGULATION
DEVELOPMENT
Private technology company
National-level Contract Law
RAS/LAWS TESTING
Armed Forces
Private technology company
International Humanitarian Law
DEPLOYMENT
Armed Forces
UPDATES & FURTHER TRAINING
Private technology company

Source: H. Corsini and L. Tybäck (2021)

However, autonomous systems' autonomy is only one essential component contributing to this new age of warfare. What other aspects must be accounted for to understand this technological transformation taking place? How do the systems that are developing these weapons differ from the previous era? Finally, why does this revolution have the potential to fundamentally change the military sector? These questions will be addressed in this first section of this report.

CIVILIAN-DRIVEN DEVELOPMENT OF RAS

From WWII onwards, the main source of innovative new technologies came from defense companies, military research institutes, and dual-use institutes with strong ties to the military.[14] From this sector came innovations that were later adapted for civilian applications: well-known examples include the origins of the Internet (ARPANET) and satellite navigation (GPS)[15]. However, since the end of the Cold War and as a general trend worldwide, military research and development (R&D) expenditure has declined. The negative impact of these trends is becoming more evident as major weapon platforms in use for decades are coming to an end, new global tensions are rising, and in the words of one global policy expert, "countries are therefore once again seeking advanced military technologies".[16] Civilian companies, on the contrary, have taken the lead when it comes to technological innovation; this is especially true concerning advances in autonomy and machine learning capacities.[17] Much of the information and communication technologies (ICT) which have significantly changed modern lives over the past several decades has emerged as the result of commercial interests. In a nutshell, a new generation of technology is principally driven by private-sector investment.[18]

This shift has two intertwined consequences: first, the military sector is increasingly interested in sourcing innovations from the civilian one[19] – especially as military planners are aware of the civil sector's lead in developing AI and autonomous systems[20]. In other words, "it can be said that RAS in the military context is developed in a 'spin-in' environment, whereby the civil domain leads in innovation".[21]

There are two separate uses for AI and autonomous technology in the military field: the former can be incorporated into the weapons themselves as well as to carry out operational missions, while the latter can be used to analyze large amounts of raw data to find targets[22]. Second, a significantly more diverse range of stakeholders is increasingly involved in the development of RAS at the military level: demand is created for interaction with designers, developers, and manufacturers outside the traditional defense industry[23], including start-ups and big technology companies which are relative newcomers to the sector[24].

RAPID DEVELOPMENT CYCLES FOR RAS

Another difference with previous military technological innovations lies in the pace: previous innovations' development cycles were measured in years – and sometimes even in decades. This created a closed environment in which only a few established contractors could realistically compete for contracts[25]. Today, not only the range of actors involved is expanding (as described above), but due to the rapid cycle of innovation RAS demand (a) fast-paced procedures both in their development and acquirement, (b) have a much shorter period of use, and (c) need to be modified, updated, inserted, or exchanged throughout their life cycle[26].

ETHICAL AND LEGAL IMPLICATIONS OF RAS AND LAWS

As we have become increasingly aware, when introducing autonomous systems it is fundamental to not only address technical and social implications, but ethical and legal ones, too – especially when these systems are used for lethal purposes. Some general examples of related questions have already been mentioned in the introduction. Private technology companies have voiced their further concerns, the latest example of which was through an open letter to the UN Convention on Certain Conventional Weapons (CCW) in 2017. In this letter, over 100 CEOs of technology companies (including SpaceX and Tesla Motor's Elon Musk) implored the UN to take actions against developing LAWS while simultaneously offering their technical advisory services, arguing that once LAWS are developed, "this Pandora's box... will be hard to close"[27].

When reviewing legal guidelines of ethical concerns around armed conflicts, one is confronted with the so-called 'Martens Clause' (also known as the dictate of public conscience) from the preamble to the 1899 Hauge Convension–I – Laws and Customs of War on Land, which states that the fact that there is no law prohibiting the use of a certain weapon does not automatically mean that its use is permitted. Why must this be explicitly stated? Because there are ethical aspects of such innovation that need to be taken into account before it may be considered appropriate for use in armed conflicts. In other words: the use of a weapon is also associated with its societal and ethical acceptance.

In the specific case of LAWS, a few proponents have argued that it is a moral obligation to develop them if they allow the reduction of harm (e.g., robots do not kill out of anger, hence they are more ethical)[28]. However, counterpoints aside, arguably the major ethical question present with LAWS is whether we can delegate the decision to kill a human being to an algorithm[29]. The implications are significant: would this undermine our very notion of humanity? Could this be considered an affront to human dignity? The political sentiment of ethical repulsion towards LAWS extends to the population of several states. According to an IPSOS poll commissioned by "The Campaign to Stop Killer Robots" in 2018, 61% of survey respondents in 26 countries were opposed to usage of LAWS.[30] This figure is up from 57% in 2017[31].

From a legal point of view, the main concern is LAWS' compliance to International Humanitarian Law and its three fundamental principles: distinction, proportionality, and precaution. Describing them in detail goes beyond the scope of this report – however, they can nurture our understanding of the underlying ethical challenges LAWS pose to all stakeholders involved in their development and use. The principle of distinction (or discrimination) refers to the necessity to discriminate between combatants and civilians at all times. Proportionality restricts the amount and kind of force used in a conflict in regard to both civilians and civilian objects, with respect to the direct anticipated military advantage. Finally, the principle of precaution states that parties involved in an armed conflict must take all feasible precautions to protect the civilian population and objects under their control against the effects of an attack[32]. Following these, in 2017, 28 prominent states argued that there should be a requirement to have some form of human control over all weapons[33]. Of note is that advocates on this list included China, who is not directly opposed to developing the required technology but is against their usage[34] – a seemingly contradicting viewpoint that highlights the difficulty of separating fast-paced technological advancements in Artificial Intelligence and Big Data from a wide variety of ensuing applications, including LAWS. Once opened, Pandora's Box will indeed be hard to close.

As noted above, in addressing ethical and legal implications of LAWS we must also question related technological and social implications. International Humanitarian Law is a legal cornerstone which seeks to regulate the conduct of war, taking into consideration fundamental shared beliefs regarding humanity and the mitigation of human suffering. Is an autonomous machine capable of understanding and complying with the three principles of IHR at all times, much less one designed for lethal purposes?

Answering this question poses a unique challenge with wider implications towards our understanding of not only ML technologies but also global humanitarian beliefs, since the interpretation of International Humanitarian Law itself is highly dependent on the context. Given this complexity, how can an algorithm balance expected civilian casualties relative to direct military advantage? Is it appropriate to delegate the responsibility of valuing a human life to a black-box RAS, whose inner decision-making processes are often not even understood by its own creator(s)?

affected by the fact that some systems have multiple purposes, i.e., both offensive and defensive (ibid).

[14] *Maaike Verbruggen, 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems' (2019) 10 Global Policy 338.*

[15] *Mihkel Jõhvik, 'Don't Be Evil' (2019).*

[16] *Verbruggen (2019).*

[17] *ibid.*

[18] *Jõhvik (2019).*

[19] *Verbruggen (2019).*

[20] *Jõhvik (2019).*

[21] *Bianca Torossian, Frank Bekkers and Klaudia Klonowska, 'Effective Stakeholder Cooperation during the Lifecycle of Robotic and Autonomous Systems' (2020).*

[22] *Jõhvik (2019).*

[23] *Torossian, Bekkers, and Klonowska (2020).*

[24] *Jõhvik (2019).*

[25] *Eric Gons and others, 'How AI and Robotics Will Disrupt the Defence Industry' (2018). Available: http://k1.caict.ac.cn/yjts/qqzkgz/zksl/201804/P020180426375927121069.pdf (accessed 18/12/20)*

[26] *Torossian, Bekkers, and Klonowska (2020).*

[27] *Future of Life Institute, 'An Open Letter to the United Nations Convention on Certain Conventional Weapons', (2017). Available at: https://futureoflife.org/autonomous-weapons-open-letter-2017/?cn-reloaded=1 (accessed 18/12/20)*

[28] *Righetti and others (2019).*

[29] *ibid.*

[30] *Human Rights Watch, 'Poll Shows Strong Opposition to 'Killer Robots' (2019). Available at: https://www.hrw.org/news/2019/01/22/poll-shows-strong-opposition-killer-robots# (accessed 18/12/20)*

[31] *ibid.*

[32] *Righetti and others (2019).*

[33] *Jõhvik (2019)*

[34] *Frank Slijper, Alice Beck and Daan Kayser, 'State of AI' (2019). Available at: https://ritholtz.com/2018/10/state-of-ai/%0AC:%5CUsers%5Clegars%5CDocuments%5CPDF LIBRARY%5Cstorage%5CNMLVIXI9%5Cstate-of-ai.html (accessed 18/12/20)*

EMERGING CHALLENGES

SECTION 2: UNDERSTANDING CORE TENSIONS FOR PUBLIC-PRIVATE PARTNERSHIPS

OVERVIEW

As we enter this new age of warfare, the rapid and growing development of technological innovations around Artificial Intelligence and Big Data in the private sector requires private companies to make important choices regarding the usage of their technology. In this section, we will address questions related to how organizations may decide to engage. What are the challenges that all stakeholders involved in the use of RAS in the military field face? What does this mean for future collaboration between private technology companies and armed forces?

TECHNOLOGICAL DEVELOPMENTS AND THEIR (NON-CIVILIAN) USE

As many technologies originally developed in the private sector have grown more attractive to the military, it has also become increasingly important for companies (both start-ups and 'big tech' alike) to be aware that their products can and will be used for non-civilian purposes. These technologies encompass all progress in the area of artificial intelligence, and include as varied areas as machine learning, cloud computing, pattern recognition , but also hardware (e.g., supercomputers to process large amounts of data) and autonomous aerial systems (i.e., drones)[35].

While primarily designed for defensive purposes, RAS systems are the basis upon which AWS (in their lethal declinations) are grounded. The civilian development of many RAS technologies serves to emphasize how boundaries between civil and military research on technology is becoming increasingly blurred, with tech companies needing to decide if – and to what extent – they want to participate in further blurring these lines, or if they will reaffirm where they believe boundaries should be.

Given the increasingly centrality of their products in the evolution of warfare, tech companies are, and will continue to be, heavily encouraged to collaborate with the military. For instance, funding and forging strong relations between tech firms and the department of defense is a focal point of American AI strategy. Encouraged by the Pentagon, in 2018 the Defense Advanced Research Projects (DARPA) budget committed to spending USD $2B over the next five years to develop advanced military AI technology[36]. This total includes funding for research projects led by specific private firms of interest to DARPA. Like DARPA in the United States, China also created a Defense and Technology Innovation Rapid Response Group in March 2018 to promote civil-military cooperation. Their aim is openly stated as using military and civilian collaboration to create AI technology to serve military purposes. Similar measures have been taken by other countries, including the UK, France and South Korea.

[35] *Jõhvik (2019)*

[36] *Slijper, Beck and Kayser (2019)*

A SHIFTING GEOPOLITICAL BALANCE OF POWER

Since the late 20th century, the United States has held the title of the strongest military power in the world. However, developments in LAWS & are arguably decreasing the power gap between America and contesting nations[37]. There is a clear link between security, military spending and investments in AI: indeed, it is no coincidence that the key states developing their AI sectors – namely, the United States, China, Russia, the United Kingdom, France, Israel, and South Korea[38] – are those in the top 10 of military spending worldwide (with the exception of Israel)[39].

This situation has led to a US struggle to maintain military superiority, as well as a scramble by other nations to gain the technological upper hand. One illustrative example is in the development of so-called anti-access technologies. Anti-access technologies include "long-range air defense systems and precision strike weapons"[40] which make it difficult for the United States' military to effectively deploy their weapons. Anti-access technologies have been developed by several states, many of which are also actively investing into and further developing their AI technology within the civil sector[41]. The previously mentioned recent Nagorno-Karabakh conflict exemplifies how superiority in systems applying AI to the military sector can decide the winner of a war. Continued international investment in civil sector-led advancements in Artificial Intelligence and Big Data technologies outside of the United States may thus also shift the balance of military power away from the US, further altering geopolitical relations at the international level.

QUESTIONING ACCOUNTABILITY: NETWORKS AND MACHINES

The use of LAWS poses many relevant legal questions especially within the scope of IHL, including who will be accountable for war crimes resulting from the use of these weapon systems. On one hand, it appears clear that there would be a strong sense of injustice if a machine, but no person, were held accountable for such actions and punished. Accountability "requires those who are responsible for their actions to be held answerable for them," frequently with the additional intent of preventing further harmful actions from taking place[42]. However, in practice this is quite challenging, as LAWS transform hierarchical organizations like the military into networks of machine-human teams, where human commanders define mission parameters and then delegate the authority to carry out missions to operators. Hence, the networked nature of command and control means that lines of accountability can and do become diffuse[43].

More generally speaking, it is the very notion of accountability which is challenged when private entities become involved in the creation and dissemination of new technologies for use in armed conflict. This is because RAS operate based on the parameters and functions which have been set by private actors, while IHL is based upon the principle that only states have 'the exclusive legitimacy to exercise violence[44]. Such 'messiness' of locating accountability brings to the forefront how the revolution posed by the Age of Autonomous Systems may even force us to reconsider our understanding of the fundamental units which comprise society, as the consequences of these technological developments outstrip the foundational scope of possible actors on which our existing legal structures from the 19th and 20th centuries were built.

[37] Gons and others (2018).

[38] As well described in the PAX report 'State of AI', which outlines the involvement of these seven key states in developing their AI sectors (see Slijper, Beck and Kayser, 2019).

[39] Iman Gosh, 'Mapped: The Countries with the Most Military Spending,' Visual Capitalist (2020). Available at: https://www.visualcapitalist.com/mapped-the-countries-with-the-most-military-spending/ (accessed 18/12/20)

[40] Gons and others (2018).

[41] ibid.

[42] Koppelman (2019).

[43] ibid.

[44] Torossian, Bekkers and Klonowska (2020).

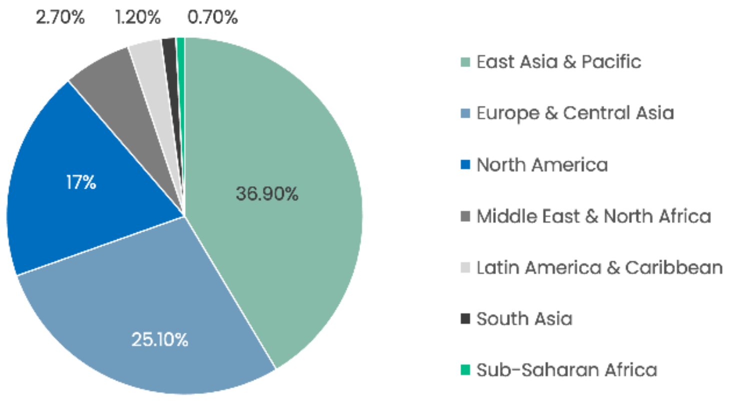


FIGURE 2. PEER-REVIEWED AI PUBLICATIONS BY REGION (2019)

Regions in descending order; Source: Stanford Institute for Human-Centred Artificial Intelligence, 2021 AI Index Report

THE PROBLEMS OF PROLIFERATION

Another issue raised when considering LAWS is that of the ease of their proliferation. Due to the complex nature of these systems combining hardware and software, it is possible to purchase individual components (e.g., drones) from the internet and other commercial sources and combine them to create potentially lethal weapons for relatively cheap, which could then be used by nonstate armed groups or terrorist organizations operating outside of IHL[45]. Control is complicated even further because of the rapid advancement in digital sharing and storage possibilities, as illustratively surfaced in recent tensions surrounding the sharing of files used for 3D printing weapons – when and how should transfers of software and technical data be limited?[46]

In a related manner, states may also transfer RAS elements to third countries without the approval of production partners, or private companies might re-sell or re-use RAS after the expiration of a contract[47]. However, tech companies can expect that governments will try to keep cutting-edge AI technology from falling into the hands of rival states. The United States provides an example of this. The official American position on AI, as stated in the 'AI Executive Order' dated February 2019 , includes promoting an international environment which supports the American endeavor into AI development, both to promote American AI industries internationally and to protect US technological advantage. This last point includes preventing key AI technologies from being acquired by adversarial states[48].

The U.S. is, obviously, not the only country seeking to cultivate and protect its AI technologies. Innovations (as indicated through related peer-reviewed AI publications and patents) for AI technologies have surged globally in recent years as seen in the figure above (Figure 2). While originally dominating both patents and peer-reviewed publications on AI-related topics, the United States' strong pipeline of academic-corporate AI collaborations has been challenged in recent years and in some instances, overtaken by innovators in Europe and China due to increased government support and resource investment. Further, given their business, geopolitical, and technological importance, AI-innovations are often heavily guarded. Fierce private and public sector legal battles (at minimum) result when attempts are made to steal or otherwise proliferate these patented technologies, even within the context of knowledge sharing among researchers and developers. Such responses serve to heavily discourage many tech companies from selling their technologies abroad, reinforcing geopolitical boundaries and preventing collaborations with private and public sector actors from certain nations.

[45] Meier (2019).

[46] Esther Chavannes, Klaudia Klonowska and Tim Sweijs, 'Governing Autonomous Weapon Systems Expanding the Solution Space , from Scoping to Applying' (2020).

[47] Torossian, Bekkers and Klonowska (2020).

A NON-LINEAR RAS LIFE-CYCLE

A particular challenge posed by RAS technologies is how the life cycle of RAS differs from traditional weapon systems, given their reliance on integrated software that continuously evolves. Hence, even when the development phase is ended and the RAS system has been handled by external contractors, the 'handing-over' of the RAS from a developer/producer to military stakeholders does not signify that the involvement of the former is finished. In short, the development, integration, and use of RAS is not linear, "due to its evolving nature which requires an iteration of military requirements, review of technical parameters and regular adjustments to allow for technological progress and new operational insights to be reflected in the system and its actual use"[49]. The complexity of these stakeholder relationships is a direct result of the RAS technology development and refinement processes themselves. This creates a variety of unique and pressing challenges, ranging from questions about delineating exclusive ownership by a single stakeholder (e.g., potentially creating conflict of interests) to further updates performed by contracted developers clearly reflecting the requests of military stakeholders[50].

BALANCING MARKET COMPETITION WITH CLOSE PPPs

A further challenge for all stakeholders engaged in the development of RAS is in finding a balance between cooperation with reliable and trustworthy partners and the management of new, innovative technological supply from competitors. Here, a risk for military stakeholders is that long-term arrangements might create a high dependency on a single technology provider with essential, proprietary knowledge resources, who may use this capture to increase their rates, lower quality, and minimize effective oversight. Because of this, it is particularly important for military stakeholders to be able to change partnerships in case of poor performance: as experts from The Hague Center for Strategic Studies have emphasized, the existence of an 'open' market may be especially salient for this new era of warfare[51].

In recent years, larger tech firms with military contracts have also increasingly engaged in segment retreat as they seek to consolidate their products and services in key areas, opening space for new companies and startups to contract with the military[52]. As an illustrative example, within the United States' 2017 Fiscal Year President's Budget, "more than 60% of the robotics-focused contracts… were awarded to nontraditional defense players or small prime contractors,"[53] potentially suggesting strong offerings beyond existing firms. With states likely to continue increasing AI investments over the coming decades, the challenge remains for both military and private tech sector stakeholders as to how to balance healthy market competition with close and effective ongoing PPPs.

OUTSOURCING AND INTEROPERABILITY

While outsourcing to third-party contractors is a common practice for developers in the age of RAS , doing so creates rather significant challenges with wide-ranging effects. First, the use of black-box machine learning processes (MLP) within RAS means that end-users (namely operators and commanders in the armed forces) do not know how a machine has learned, nor how it has created its own learning patterns. This, in turn, limits predictability in the possible outcomes of an RAS in the battlefield[54]. Second, interoperability with other allies' RAS technologies can be complicated as military forces might need to operate RAS they have never worked with, and which might have been developed by entirely different private companies[55]. Finally, there exists a widening knowledge gap between technical and technological experts and other stakeholders involved in the life cycle of RAS that is further exacerbated by the outsourcing of research and production of military technologies to private actors[56]. These challenges represent only a few of those created by third-party outsourcing, though serve to capture broader trends including (a) the ongoing siloing of expert knowledge separate from end users and (b) increasing interoperability concerns across national boundaries.

[48] *Slijper, Beck and Kayser (2019).*

[49] *Torossian, Bekkers and Klonowska (2020).*

[50] *ibid.*

[51] *ibid.*

[52] *Jõhvik (2019).*

BIG DATA AND MACHINE LEARNING

Data play a crucial role for RAS, as they are needed to train the algorithms to perform specific tasks in an unpredictable environment. The modern military is drowning in data, which could be seen as an advantage in the development phase. However, it also represents a challenge, as it is not always labelled, properly formatted and freely accessible to developers. Even though it is indeed possible to train algorithms with unlabelled data, it increases unpredictability and makes it harder to explain outcomes[57]. On a similar note, data sets (because of privacy issues or sensitivity) sometimes cannot be from real-life situations, which makes training RAS even more difficult.[58]

This is also relevant in the context of legal questions on LAWS and their compliance with IHL: How will a machine behave when something unexpected happens? Will it be capable of accurate situation assessment at all times? This in turn determines predictability, and hence the guarantee that LAWS comply with IHL principles in the battlefield at all times. Being able to predict the way in which a machine will behave in unknown circumstances is largely dependent on its learning processes as well as the data used to program it.

BRIDGING DIVERSE ORGANIZATIONAL CULTURES

Finally, the military is well known for its strong hierarchical organizational and management structure, where roles are clearly defined and authority rests within an explicit chain of command.[59] This structure can contrast greatly with modern private sector organizational cultures, and especially that of tech companies and start-ups where flat organizational hierarchies are not uncommon. Research has repeatedly demonstrated that the resulting differences in organizational culture are likely to provoke tensions[60], as collaborations between these two "worlds" may require negotiating (among other items) fundamentally different timescales, flexibility in approaches to work, managerial openness to feedback, responsiveness to organizational traditions, perception of organizational mission alignment, etc.

[53] *Gons and others (2018).*

[54] *Koppelman (2019).*

[55] *Chavannes and Arkhipov-Goyal (2019).*

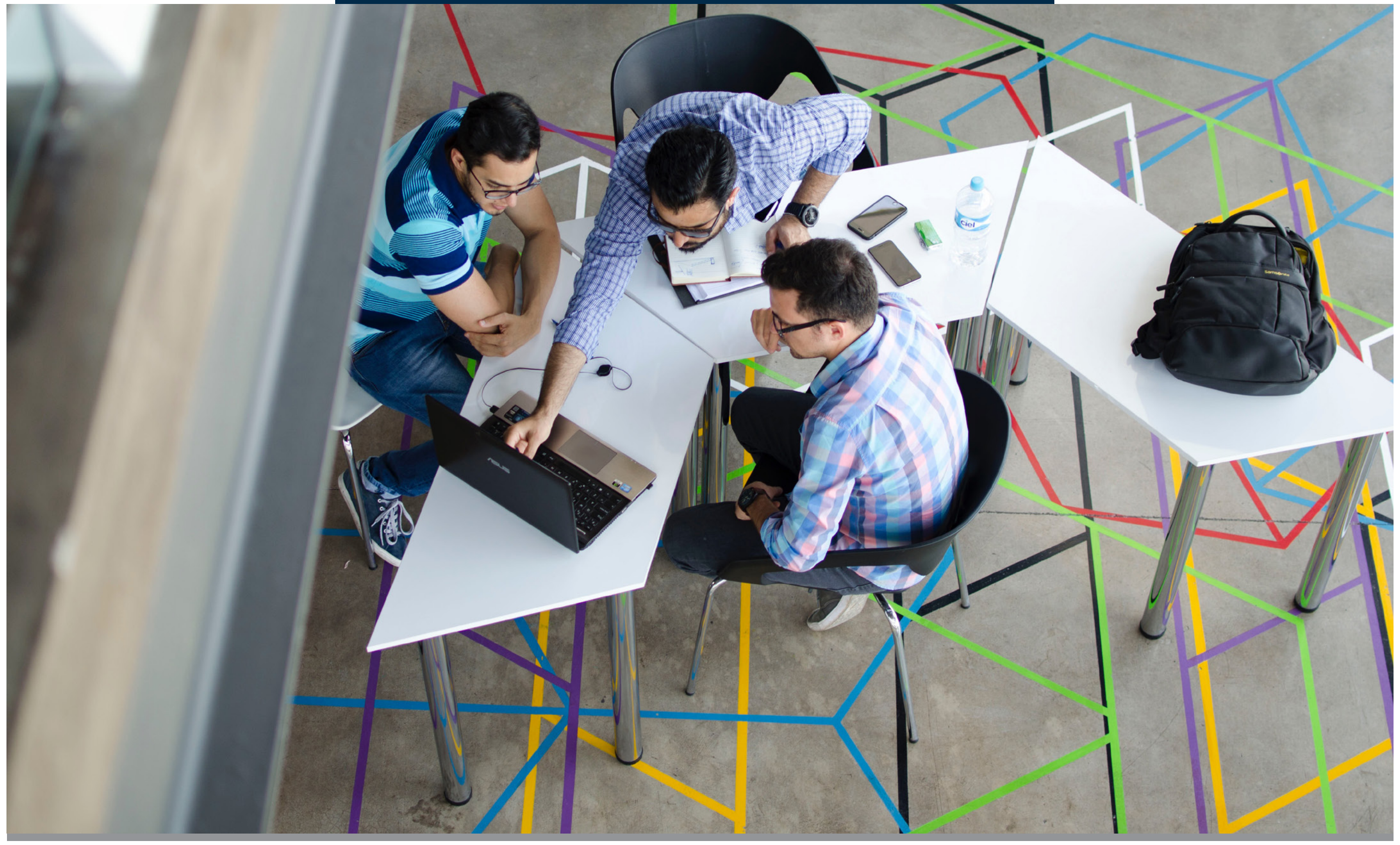
[56] *Chavannes, Klonowska and Sweijs (2020).*

[57] *Verbruggen (2019).*

[58] *Koppelman (2019).*

[59] *Joseph L. Soeters, Donna J. Winslow, and Alise Weibull, "Military Culture," (2007) Handbook of the Sociology of the Military, p. 237-254.*

[60] *E.g., Daniel R. Denison and Aneil K. Mishra, " Toward a Theory of Organizational Culture and Effectiveness," (1995) 6 Organization Science 204; Roberto A. Weber and Colin F. Camerer, "Cultural Conflict and Merger Failure: An Experimental Approach," (2003) 49 Management Science 400.*



STAKEHOLDER RECOMMENDATIONS

SECTION 3: KEY ACTION AREAS

Based on the unique challenges posed by the Age of Autonomous Systems to civilian-military cooperation, this section elaborates three key action areas (consisting of eight specific recommendations) for civilian technology company stakeholders to consider when debating engagement with the development and deployment of RAS for military use and more specifically, LAWS.

ACTION 1:
IMPROVE STAKEHOLDER TRUST AND COMMUNICATION CULTURE

BUILDING TRUST IN LONG-TERM PPPs

Clear communication is the first step in establishing an atmosphere of trust among the various stakeholders involved in RAS and LAWS development. This can be further supported through the creation of meaningful, long-term private-public partnerships throughout the phases of the RAS development lifecycle. Such long-term trust is particularly relevant given the need for developers to re-engage with RAS products following their deployment, as until such a point as these skills are internalized within military capabilities, these developers' technical expertise is needed to update, modify, refine, and advance these technologies based on new training data and results.

A clear division of tasks and responsibilities between stakeholders – as must be stated in these public-private partnership contracts – will be critical. At the same time, clauses should be integrated stating when and under which terms cooperation can be terminated (e.g., in case of ill-performance[61] or non-achievement of specific targets discussed at the beginning of the development phase). Clarity of communication, both between stakeholders and within technology companies themselves, will be critical to successfully achieve and maintain an appropriate level of long-term trust.

PRIORITIZING COMMUNICATION CULTURE

With the wide variety of stakeholders now required to facilitate the many steps of the RAS life cycle, it is vital to create a strong communication culture. This is relevant for several issues: for the military, to describe their needs; for policymakers, to give legal knowledge and ensure compliance of these systems to IHL; and for private companies, to transparently present the limits of their technological capabilities. All of these must be integrated in the functional and technical parameters of RAS.[62]

Furthermore, prioritizing the maintenance of a clear communication culture may assist in overcoming possible tensions between stakeholders caused by radically different organizational and managerial cultures (e.g., between hierarchical military customers and non-hierarchical civilian technology develoment organizations). At each stage of the RAS life cycle (i.e., development, integration, use, and re-training) it will be essential for actors from multiple fields to come together to negotiate goals, set partnership parameters, and discuss the performance and limitations of the RAS and LAWS technologies being developed.

[61] *This is presented, among others, in the report by Torossian, Bekkers, and Klonowska (2020). However, what the authors do not describe is the way in which such a communication could be put into practice.*

[62] *ibid.*

ACTION 2:
ESTABLISH CLEAR BOUNDARIES AND ACCOUNTABILITY

APPROPRIATELY TRAIN MILITARY PERSONNEL

Military personnel interacting with RAS must be confident and have an informed trust in the machine, facilitated by their understanding of how it will react in unknown environments. It is the developers' duty to ensure that the technology is sufficiently transparent with its limitations clearly understood by end-users. These training requirements should be clearly stated within the terms of the contract established between the involved parties. From a legal point of view, it is only the state that can use force legitimately; thus, at least until there exists a legal framework directly targeting the governance of LAWS, the authors believe that the responsibility and accountability of maintaining adequate end-user training is that of the military. Hence, it is important for commanders and operators alike to recieve sufficient technical knowledge and training to understand the abilities and limitations of these systems with which they will be working in the field.[63]

ESTABLISH CLEAR CODES OF CONDUCT

Establishing clear codes of conduct are another important element for civilian technology companies in delineating their engagement with RAS and LAWS development, as they allow stakeholders to create manuals directly linking technological requirements to military objectives. Such codes might also include details specifying the responsibilities of the involved parties at each stage, as well as highlighting improvements and potential operational shortcomings.[64] Moreover, such codes could be used as the basis for addressing subsequent additional issues, including the use and quality of data for MLP or the re-use and/or re-selling to other countries of the developed technology after the initial contract ends.

Especially when considering possible proliferation, it is essential for international security purposes not to leave ownership of LAWS technologies exclusively with the developer. For such security-sensitive issues, it is important that the control of LAWS remains in the hands of the military (and the state, by extension). This matter is particularly relevant given that Article 36 of Additional Protocol I of the 1949 Geneva Conventions imposes an obligation on states to conduct a review for all new weapons to determine if their use would be in all (or some) circumstances prohibited by IHL.

DELINEATE PPP BOUNDARIES PRIOR TO COLLABORATION

For private, civilian technology companies, it is important to realize that developing dual-use technologies also means that there is a real possibility that such technologies might be co-opted for non-civilian purposes. Ethical questions thus need to be addressed ***before*** entering into any partnerships with military programs towards RAS development, and particularly when there is a possibility of the technology being used as a LAWS. For instance, in 2018 thousands of Google staff signed an open letter calling for an end of the company's collaboration with the United States' Pentagon on Project Maven (where Google-developed AI was used to interpret video images, which could provide the basis for automatic targeting and LAWS). Following this letter, Google did not renew its contract and also published ethical AI principles, stating that Google will not design or deploy AI in weapons or other technologies whose purpose or implementation is to cause or facilitate injury to human beings.[65]

Examples of such propositions can include: (1) commiting publicly to not contribute to the development of LAWS; (2) establishing clear organizational policies stating this commitment (e.g., through the assessment of each new project by an ethics committee, the analysis of all technology developed and its potential uses and implications, the addition of a clause in contracts stating that this technology should not be used for LAWS, etc.); and (3) ensuring that employees are well informed through an active culture of transparency while management also remains open and responsive to employee concerns.[66]

Even with these clear internal boundaries, however, the authors do not believe that it is possible to impede the spread of dual-use technologies to the military sector. If ethical concerns become an obstacle to cooperation between private technology companies and armed forces, AI developers should ensure that the existing technologies are reliable, predictable, and safe for the military to be used in real-world environments (e.g., through AI solutions to appropriately analyze data, or via the technological training of military personnel – see prior recommendation). Moreover, it may be in technology companies' best interests to support military personnel in achieving a greater degree of technological independence, and to cultivate the internal capabilities to develop these technologies further. Such actions would thus ensure that the legal responsibility of LAWS is clearly in the hands of armed forces, and more generally, the state. However, such independence also poses potentially significant oversight concerns if no enforcible, third-party mechanisms to serve as a checks and balances are introduced to govern the use of these lethal autonomous weapons by the military. In sum, the authors believe that for the present, the boundaries of private-public partnerships must be transparent and clearly established prior to collaborations in the future.

BALANCE TRADE-OFFS OF MILITARY FUNDING

Smaller, privately held technology companies face different funding challenges than large, established military contractors that do not need to defend a dominant position in the market. Leadership within smaller firms must thus carefully consider the trade-offs between accessing (often significant) funds provided by the military and the ethical reasons they may have to refuse entering into such an agreement. In making this choice, there are several possible strategic consequences the authors recommend that leadership take into account (including but not limited to):

(1) the availability of other potential funding opportunities;

(2) potential loss in revenue from public boycotts and reputational damage from engaging in the development of RAS (and by extention, possibly LAWS);

(3) potential opposition from employees within the company; and

(4) restrictions and requirements connected to military funding.

If the leadership of a civilian technology company chooses to move forward in engaging with the military in the development and deployment of RAS, we strongly recommend that both partners establish a clear code of conduct with delineated boundaries of responsibility and accountability (as previously mentioned in this report). We also recommend that leadership keep in mind that the military, if they see it as imperative, may also use your technology for LAWS despite previous agreement.

[63] This is similar to the non-legal (i.e., technical) solutions proposed by Chavannes, Klonowska and Sweijs (2020).

[64] ibid.

[65] Jõhvik (2019).

[66] ibid.

ACTION 3: PROACTIVE MANAGEMENT OF DATA, DATA ANALYSIS, AND FURTHER TECHNOLOGICAL DEVELOPMENT

MILITARY-BASED MANAGEMENT AND ANALYSIS OF DATA

As previously discussed, modern military stakeholders have access to a large volume of raw data. However, this data presently can only be used to train algorithms with a degree of difficulty, as much is unstructured and/or stored across unintegrated databases. However, machine learning has advanced in such a way that some datasets can already be analyzed through automated processes.[67] It is the view of the authors that private civilian technology companies have the opportunity to share this technology with the military, not only for the purposes of exploiting this large amount of data for military (rather than civilian-based) testing and re-training of the algorithms after their use in the battlefield, but also to allow the armed forces to independently manage sensitive security data which should not be shared with third parties.

PROVIDE IT-SOLUTIONS FOR 'MEANINGFUL HUMAN CONTROL'

While it is not yet clear what decisions will be taken at the international level to regulate LAWS, this does not mean that developers cannot make valuable contributions to the current design of RAS (and LAWS), even before legally-binding propositions are made. This is particularly true with regards to 'meaningful human control,' a term firstly introduced by the NGO Article 36.[68] There are many different possible degrees of human oversight for LAWS mirroring levels of autonomy used in other applications, such as for self-driving cars; these range from the need for a human to deliberate and select the LAWS' target, to a machine targeting and attacking in full autonomy. Examples for what human oversight could encompass include: (a) a designated time frame allowing a human operator to veto the selected target before the machine attacks; (b) the need for active human operator approval before the machine can proceed; and/or (c) mandating that the target(s) to be attacked be depicted by the machine as a human from a list of possible targets provided by the machine.[69]

Each of these options need to be evaluated carefully based on further scientific evidence regarding human-machine teaming, as well as the context in which LAWS may be deployed. Operational experience shows that sustaining vigilance as a passive supervisor can be quite challenging for people (for instance, only reading data provided by the machine would be considered a passive action for human operators and has been demonstrated to cause significant issues in autonomous vehicle operation). If a system is deployed far away from civilians (e.g., in the middle of the ocean), it may be more acceptable to leave full autonomy to the machine.[70] Ultimately, is up to developers in the IT sector to identify and provide evidence-based, concrete solutions allowing meaningful human control. Through a constructive dialogue with the end-users, private companies can already think about introducing into their systems mechanisms including timeframes for veto, final feedback-loops to the human operator, etc. In a sector where creativity and innovation are among the strongest assets, these strengths can be used to find innovative solutions even before decisions at the international level are taken about LAWS and the parameters of their legality.

[67] *Greg Allen and Taniel Chan, 'Artificial Intelligence and National Security' (2017).*

[68] *Righetti and others (2019).*

[69] *Koppelman (2019).*

[70] *ibid.*

CONCLUSION
& SUMMARY

Lethal Autonomous Weapons Systems (LAWS) and Robotic and Autonomous Systems (RAS) already exist, are being deployed in modern combat, and are now an important part of the future of warfare.

As such, constructive debate about the challenges (as well as the opportunities) that this new reality brings upon us is key. Within this GDI report, we have sought to consider the perspective of private, civilian technology companies (including "big tech" and start-ups alike) involved in the development of RAS, and more clearly outline the core tensions that arise from their engaging in technology development partnerships with the military sector. With the execption of a few papers and reports[71], the majority of documents published on RAS and LAWS have remained addressed to politicians and officials in international organizations (such as the UN) and focused on highlighting possible geopolitical consequences, or pleading for legal regulations. Even when directly addressing private, civilian technology companies, the central premise of these reports remains focused on either moral and ethical-based calls for organizations to 'not to be evil'[72] by engaging with these technologies, or extortions to not to lose (as established contractors) ther market share to younger and more dynamic technology 'newcomers'[73].

The authors of this report, however, believe that it is beyond time to consider this revolution in warfare in a different manner. Starting from the challenges that big data and advances in Artificial Intelligence pose to private-public partnerships, we have discussed possible recommendations to be adopted by civilian technology companies in their role as key stakeholders now embedded within ongoing processes of RAS (and by extension, LAWS) development. These recommendations can be intepreted as tools for guiding successful PPP collaborations, but also as an opportunity for leadership to deeply consider what the decision of engaging in such a relationship might entail.

Given that the use of LAWS in modern warfare is already a reality, the authors of this report firmly believe that it is vital to move the discussion of LAWS beyond stigmatizing images or opaque expert discussions of the technical elements involved in RAS development. Instead, we argue that we must enter this new era of warfare with an open mind; a systems-level perspective of the LAWS development, production, and refinement processes; and the knowledge key for stakeholders to make informed decisions – in whichever direction this may this be.

[71] *For instance: Jõhvik (2019), Gons and others (2018), Torossian, Bekkers and Klonowska (2020), Chavannes, Klonowska and Sweijs (2020).*

[72] *Jõhvik (2019)*

[73] *Gons and others (2018).*

02

GOOD DATA INITATIVE

© 2021 Good Data Initiative

Email
hi@gooddatainitiative.com

Website
www.gooddatainitiative.com

Phone
+44 75 8888 7300