Assessing Autonomous Weapons as a Proliferation Risk
The Future Has Not Been Written

Paul O’Neill, Sam Cranny-Evans and Sarah Ashbridge
193 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 193 years.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2024 by the Royal United Services Institute for Defence and Security Studies.

© RUSI, 2024

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, February 2024. ISSN 2397-0286 (Online).

Cover Image: Mariusz Burcz / Alamy Stock Photo
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Methodology</td>
<td>4</td>
</tr>
<tr>
<td>I. Understanding LAWS</td>
<td>6</td>
</tr>
<tr>
<td>Military Interest in LAWS</td>
<td>7</td>
</tr>
<tr>
<td>Policy Framework</td>
<td>9</td>
</tr>
<tr>
<td>Regulation to Control Proliferation</td>
<td>11</td>
</tr>
<tr>
<td>II. Minimum Viable Product LAWS</td>
<td>13</td>
</tr>
<tr>
<td>Individual MVP Use</td>
<td>13</td>
</tr>
<tr>
<td>Armed Forces’ MVP Use</td>
<td>15</td>
</tr>
<tr>
<td>III. Military Off-the-Shelf LAWS</td>
<td>17</td>
</tr>
<tr>
<td>China</td>
<td>18</td>
</tr>
<tr>
<td>Iran</td>
<td>19</td>
</tr>
<tr>
<td>Israel</td>
<td>20</td>
</tr>
<tr>
<td>Russia</td>
<td>21</td>
</tr>
<tr>
<td>Turkey</td>
<td>22</td>
</tr>
<tr>
<td>The UAE</td>
<td>23</td>
</tr>
<tr>
<td>IV. Boutique LAWS</td>
<td>24</td>
</tr>
<tr>
<td>V. Proliferation Constraints</td>
<td>28</td>
</tr>
<tr>
<td>Conclusion</td>
<td>33</td>
</tr>
<tr>
<td>About the Authors</td>
<td>35</td>
</tr>
</tbody>
</table>
Executive Summary

The proliferation of systems that can provide lethal autonomy is inevitable, given both the availability of the (often dual-use) technology that underpins lethal autonomous weapon systems (LAWS) and the benefits that such systems are seen to bring to some users. LAWS will cause problems for armed forces, but the absence of an agreed definition complicates attempts to regulate and control their proliferation.

LAWS are not a single capability. Hence, this paper considers the risks associated with LAWS based on the likelihood and impact of their proliferation in relation to three broad categories: minimum viable product (MVP); military off the shelf (MOTS); and boutique. The sophistication of these systems differs significantly, as do the risks each pose and the demands they place on users, all of which has an impact on the proliferation risk.

MVP LAWS involve homemade and commercially specified and available technologies. The software, hardware and expertise necessary to develop a minimally functioning LAWS are widely available and within the reach of non-state actors if they see benefit in its adoption. These weapons represent the biggest risk of proliferation, especially in relation to non-state actors, but they are often fragile and, considered individually, are not game-changing (in terms of impact) for modern militaries. However, even relatively simple systems used at scale can still cause problems for Western militaries, who often lack mass.

MOTS have high degrees of autonomy and are proliferating rapidly to anyone with sufficient funds, including non-state actors. However, while many are offensive capabilities, they also include defensive systems, such as air defence weapons that are often autonomous but not offensive. The risk posed by MOTS LAWS is arguably limited by affordability, but there may be clear advantages to adoption, including enabling battlefield mass. MOTS proliferation is highly likely, and military advances in autonomy are more a matter of will and ethics than of technological hurdles. So, while the likelihood of proliferation is high (if slightly lower than for MVPs), the impact is higher, especially if the systems can be used at scale.

Boutique LAWS are exquisite capabilities being developed by a select few countries. They are very expensive complex systems designed for specific effects against well-identified threats, such as a specific element of an opponent’s strategic
defensive network or deterrence capabilities, and as such are the most destabilising (high impact). Their adoption advantage is high, but the cost of developing and maintaining them means proliferation is currently unlikely beyond the wealthiest states.

Adoption advantage is needed for LAWS to proliferate and, in many areas, such as the MVP and MOTS paradigms, advanced conventional capabilities still have an edge over LAWs, although this may change. As the technology underpinning LAWS matures and becomes proven, proliferation risks will increase. Militaries have the opportunity, and arguably the responsibility, to lead the conversation about proliferation and shape its outcomes.
On 14 September 2019, 25 drones and missiles in two waves damaged the Abqaiq and Khurais oil-processing facilities in Saudi Arabia, evading the advanced air defence systems guarding them.¹ This was not the first attack on the Abqaiq facility. In 2006, Al-Qa’ida had used humans and vehicle-borne improvised explosive devices (VBIED), but the assailants were discovered by guards and killed, and the facility was not damaged.² The two attacks, 13 years apart, highlight the pace at which technology has evolved, and how easily it can be wielded against states that previously enjoyed technological supremacy. The 2019 attacks were reportedly facilitated, and possibly launched, by Iranian forces using weapons developed for asymmetrically challenging regional opponents.³ Nonetheless, capabilities that were previously the preserve of nation states have proliferated to non-state actors, allowing them to attack cargo ships, airports and armed forces.⁴

Non-state actors have demonstrated a willingness to adopt new and unproven technologies to create asymmetric advantage against more powerful opponents. In 2016, Islamic State (IS) forces in Mosul used UAVs to coordinate attacks against Iraqi forces using VBIEDs and mortars.⁵ Small states also appear willing to employ relatively untested technologies, such as loitering munitions and armed UAVs, to achieve their military goals. For example, in the 2020 Nagorno-Karabakh war, Azeri forces deployed loitering munitions and UAVs to prepare for conventional combined arms assaults.⁶ Forces unable to access more sophisticated capabilities offered by Western militaries may look to increase the level of autonomy of their weapons to offset the extensive targeting and strike capabilities facing them. This poses risks that need to be considered.⁷

---

This paper considers the risks of proliferation of lethal autonomous weapons (LAWS) for military organisations. Smaller, less powerful states, and non-state actors, represent a high proliferation risk via a minimum viable product (MVP) paradigm using LAWS that are rudimentary, but whose impact is medium. Military off-the-shelf (MOTS) products – ready-made weapons systems with varying degrees of autonomy – also present a proliferation risk and greater impact challenges, as they are more capable. Exquisite, or boutique, LAWS capabilities – such as the US Air Force’s Collaborative Combat Aircraft\(^8\) – have a lower likelihood of proliferation because of the cost, very high impact risk they carry, and the sophistication of the systems and organisations needed to operate them effectively. Consequently, boutique LAWS are only briefly covered here, but they are extensively addressed elsewhere, for example in Paul Scharre’s *Army of None: Autonomous Weapons and the Future of War*.\(^9\)

**Methodology**

This paper, aimed primarily at practitioners and policymakers rather than academic audiences, assesses the likely risks to Western military organisations posed by the proliferation of different types of LAWS. It relies on a review of secondary sources supplemented by interviews with leading experts. A literature review was conducted between August 2022 and April 2023 to assess the technological, regulatory and military drivers affecting the proliferation of LAWS. The review engaged widely with policy documents from NATO, the UK government and the International Committee of the Red Cross (ICRC), research documents from industry and civil society organisations, and national and international legal frameworks regulating LAWS use and development. Non-traditional sources were used (for example, blogs, YouTube) to investigate non-state developments, such as those created by lone actors. The literature review was supported by interviews with three leading experts to frame the challenges and enable further research through specialised defence media publications and academic institutions.

The paper is comprised of five chapters. Chapter I establishes a definition of LAWS and outlines the current regulatory frameworks. Chapter II introduces MVP LAWS, and Chapter III covers some existing MOTS LAWS. Chapters IV and V examine currently available boutique LAWS and consider constraints on proliferation arising from within user organisations and thus the overall proliferation risk. The conclusion reiterates the risks facing Western militaries

---


from LAWS and urges them to engage in shaping the environment through policy debates and in developing counter-LAWS capabilities.
I. Understanding LAWS

The issue of autonomy, especially involving LAWS, is complex and contested.

Even obtaining clarity on a definition is challenging, because LAWS are systems comprising many elements, rather than a specific capability that can be neatly bounded. This paper adopts the ICRC ‘position’ on LAWS, in which LAWS are systems built and programmed using software to ‘select and apply force to targets without human intervention’ once deployed. These systems may or may not employ AI-enabled software to complete their mission or determine the best course of action. This definition is admittedly minimal, because it does not necessitate a capacity for automated target discrimination. However, as this paper specifically explores proliferation risks, the definition is sufficient for considering current systems.

There are many types of lethal weapons in service that employ some form of autonomy, and that number is growing. Such systems incorporate aspects of autonomy that include navigation, targeting, lethal weapons release or a combination of these, but in policy terms, many Western militaries seek to apply ‘meaningful human control’ to decisions to release weapons; that is, they commit to maintaining a human in the kill chain who must approve the use of the lethal weapon. It is currently less common that LAWS are able or permitted to select their own targets based on neural networks, for example. Systems such as the Israeli Harpy loitering munition that attacks radar systems matching its target catalogue, or the Russian Lancet system, which is widely used in Ukraine and reputedly has similar characteristics or functions, although this is uncertain, rely on software that is hard-coded. So, even though the program that enables


this is a form of AI that conducts operations that would typically require a human brain, it does so based on software that is predictable.

The following section considers the military interest in LAWS and some of the challenges of adoption, and then considers the policy framework within which the debate about LAWS is conducted, with a brief examination of the twin-track approach to a mix of prohibition and control currently being adopted by parts of the international community.

**Military Interest in LAWS**

Autonomy plays a part in many systems that ultimately deliver lethal effect, covering the data gathering to improve the accuracy and speed of targeting, through to the weapons, such as missiles or ‘smart’ mines, that are then deployed to destroy or kill targets. Inevitably, there are risks with this, such as error in target selection, but autonomy and remotely operated systems offer militaries (and non-state actors) benefits in terms of the efficiency and effectiveness of lethality. They potentially allow for increases in battlefield mass and reduce costs – human and financial – by taking people out of the system and allowing one human to manage multiple effectors. This offers the prospect of increased mass and lethality from smaller forces, which might also help Western militaries respond to the societal, technological and political factors driving smaller armed forces. Autonomy might also reduce casualties for the side deploying such weapons by distancing them from the battlefield, even if it does not lower the total number of casualties.

Despite the potential benefits of LAWS, the mere existence of the technology is insufficient to drive proliferation, which is also impacted by factors such as organisational and technological system design and challenges of effective integration. The impetus for proliferation requires factors to combine and create value in adoption. This ‘adoption advantage’ is unique to each entity. Militaries generally have a high adoption threshold because, to varying degrees, their conventional capabilities are extensive, and they have the structures and processes to support the use of these capabilities. However, funding and power structures play a part in proliferation. The influence of regional commanders, instead of there being an overarching strategy of adoption, allegedly led to haphazard procurement of armed drones in the Saudi Arabian military. Similar stovepipes exist within other militaries, and could both lead to the rapid introduction of LAWS and hamper its effective integration into wider force design. For example, Iraq’s LAWS procurement is believed to be shaped by individuals affiliated with

---

Iran who are also trying to reduce reliance on Western arms, for whom the adoption advantage may be less about the capabilities than about the geopolitics. But institutional barriers can raise the level required for adoption advantage in military bureaucracies.

Non-state actors may have lower thresholds for adoption, especially if subjected to survival pressures by larger, well-equipped conventional militaries. State and non-state militaries are shaped very rapidly during conflict. The constant pressure of combat (losses, successes and failures) drives adaptation from the top of an organisation to the bottom, as well as from the bottom up. However, in non-state organisations, an absence of the procedures and structures typically found in militaries drives a different kind of innovation that may shape the proliferation of LAWS. Even large, seemingly homogeneous, organisations such as IS – which at one point claimed to have 31,500 fighters – comprise many smaller organisations technically working together, but often pursuing their own aims according to the local context. Thus, proliferation may be haphazard, and result in the technology’s opportunities being less well exploited.

The adoption advantage of LAWS is not absolute. Swarms of drones may be more lethal than a single drone but may not be more effective than an artillery barrage or precision strike by long-range missiles, both of which already exist in military inventories and are integrated into doctrine and tactics. Furthermore, humans still have an edge in some areas; LAWS will struggle to replace humans in counterinsurgency roles, or verify aircraft entering a country’s airspace. So, humans are likely to be better, albeit slower, combatants than LAWS in some circumstances, and current LAWS are typically better at augmenting capabilities within narrow confines, freeing humans to do other things. Nonetheless, the fact that autonomous weapons can be produced using dual-use technology, and their prevalence on the international market (both legitimate and black markets), suggests that autonomous weapons will be used by more states in the next decade. Furthermore, the war in Ukraine could accelerate this proliferation, whereby sophisticated technologies are captured and made available for reverse engineering by states or criminal actors with fewer controls on autonomous modes, their use or sale.

In peacetime, the drivers and character of military innovation and adaptation are less settled.\textsuperscript{19} Theo Farrell argues that militaries are bound by rationality and routine – more prone to exploiting existing structures, processes and technologies than to exploring new ones.\textsuperscript{20} Peacetime innovation within armed forces is, therefore, difficult, often driven by perceived changes in a state’s environment, as well as hypotheses about the changing technological landscape.\textsuperscript{21} This is likely to impact on the large-scale adoption of LAWS in many militaries. A rare example of radical peacetime innovation is the US Marine Corps’ (USMC) ‘Force Design 2030’, which moves the Corps from heavy land warfare capabilities to a lighter, multi-role littoral force supporting the US Navy.\textsuperscript{22} Under this programme, the USMC divested itself of $16 billion of proven (non-autonomous) platforms, such as the M1 Abrams main battle tank, to invest in new technologies, for example, long-range anti-ship missiles, and adopted new doctrine and concepts of operations to deter and compete with China.\textsuperscript{23} The move represents considerable organisational risk to the USMC, and may compromise its ability to fight conventional land wars, but has been justified against the potential risks to US security, especially in the Indo-Pacific. However, experience suggests that peacetime innovation that requires significant change in doctrine, tactics or technological capabilities will likely be radical and require enterprise-wide reform and, as such, is often resisted.

**Policy Framework**

Despite the tactical and operational arguments for the adoption of LAWS, there are concerns about proliferation, and the debate around the potential impact of LAWS has reached the UN. The Convention on Certain Conventional Weapons (CCW) seeks to ‘ban or restrict the use of specific types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately’\textsuperscript{24} and has been ratified by 126 states.\textsuperscript{25} However, decisions are made by consensus, achieved through ‘the absence of objection rather than a particular majority’, giving individual states the power to veto

\begin{footnotesize}
\end{footnotesize}
proposals made. In 2016, a Group of Governmental Experts (GGE) on LAWS was formed to convene military, legal, technological and diplomatic experts from the state parties, international institutions, NGOs, academia and other parts of civil society.

The CCW framework has three themes around autonomous weapons:

1. The necessity for international regulation governing the development of LAWS: 90 of the 126 states currently support a legally binding instrument with both prohibition and regulation. 26
2. How human–machine interaction will and will not inform the use of LAWS, and where human control should be applied.
3. How autonomous systems are defined and interpreted, their role within society and their use in warfare. 27

The GGE has also adopted 11 guiding principles for responsible state behaviour around LAWS, although attempts to regulate LAWS have been hindered by the inability to agree a definition of them. Consequently, consensus-based decision-making in the near future is challenging, ‘if not impossible’. 28 Individual countries can determine their own parameters for LAWS use.

The UK government, in an annex on LAWS in its Defence Artificial Intelligence Strategy, argued for ‘context-appropriate human involvement’. 29 What ‘appropriate’ meant was not specified, so while the Strategy is positive in terms of Britain’s potential to lead development of an international status quo for LAWS, the lack of clarity is similar to concerns expressed about ambiguity in other policy positions on this subject. 30

In October 2022, in the largest cross-regional statement in any UN discussions on the topic, 70 states in the UN General Assembly issued a joint statement on LAWS. The statement acknowledged serious humanitarian, legal, security, technological and ethical concerns surrounding the use of LAWS, and the need to assure structures for human accountability regarding the use of force. There was a particular emphasis on the need for internationally agreed rules, with a combination of prohibitions and regulations to limit the uses of LAWS seen as more realistic than a blanket restriction, given the lack of a clear definition of

---

the systems under discussion. Reflecting this, a joint call to develop, by 2026, a legally binding instrument setting clear prohibitions and restrictions on autonomous weapons was made by the UN secretary-general and the president of the ICRC in October 2023. This was followed by the General Assembly approving a resolution on regulating autonomous systems, which was supported by 164 states, including several major military powers.

Regulation to Control Proliferation

An outright ban on LAWS remains unlikely, given the definitional challenges, scope for dual-use technologies, breadth of LAWS applications and the potential strategic advantages for armed forces. However, regulating specific uses or consequences of using LAWS and building on existing law is plausible, and may be desirable, given the potential of LAWS to create instability. Militaries are potentially well placed to lead this, because they own their targeting cycles and can dictate what is and is not acceptable or responsible as a part of them. They could, therefore, use their influence through requirement setting to shape the international debate on LAWS regulation.

The procurement and use of autonomous systems are always subject to human decision-making; a human decided to buy and deploy the weapon. Such decisions are typically made at strategic or operational command levels in Western armed forces with legal advice, although not all users will take the same approach. Commanders will, broadly, understand the parameters of LAWS within the context of international humanitarian law, which will inform their use. Although commanders may not understand the details and complexities of specific algorithms, their position within the military organisation guarantees a level of accountability under existing legal frameworks designed to prevent negative effects for civilians and personnel. Militaries can regulate the use of LAWS further through the training of decision-making in ways that minimise unpredictability in their use and maintenance. Even where knowledge gaps

exist within a military, someone can be held directly responsible for their use. This remains true regardless of the level of autonomy or the unpredictability of any given LAWS. However, clear chains of accountability do not completely eliminate the risk of unpredictability in technology or humans, nor the risks presented by independent systems.

‘Independence’ raises important questions of specificity. LAWS will do what they have been programmed to do. Simple systems may be able to launch a strike in response to a specific stimulus – for example, a suspicious aircraft moving at high velocity within national territory. More complex systems may be programmed to self-teach using ever-expanding datasets, and have greater freedom to decide for themselves how to respond to less predefined situations. Either system could operate with or without human oversight, and both could deliver lethal or non-lethal operational advantage. The spectrum of possibilities, uses and effects associated with LAWS is already broad enough to limit the ability to prohibit LAWS, and this breadth must inform attempts to regulate their use. The specific uses of LAWS and consequences of their use will, therefore, drive attempts at regulation. This specificity will also help to mitigate the complexities of debates over the role of the human, assuming there is human interaction beyond initial deployment, and could help improve the definition of LAWS.

If the armed forces can satisfy themselves that they have taken adequate steps to consider any potential effects on civilians and have determined the outcome as necessary to achieve a strategic aim, the use of LAWS may not fall beyond the boundaries of international humanitarian law or the Geneva Conventions – regardless of the level of human interaction. These factors mean that attempts at regulation are more likely to succeed by focusing on specific outcomes rather than on the role of the human, although this remains a difficult area to navigate, and friction remains over when and how regulation should apply. In the GGE in 2023, the UK, Ireland, Norway and Switzerland, among others, promoted examination of common characteristics and effects, with flexibility to reflect the rapid pace of technological change. The US differed, proposing a focus on the objective nature of the weapons system rather than its use, but fell short of calling for international law. India, Israel and Russia explicitly stated they would not agree to a legal instrument. This block to progress is unlikely to be lifted soon, but the shift towards regulating LAWS in specific contexts could provide space to explore how existing international humanitarian law applies to specific scenarios where different types of LAWS might be used, to test the suitability of existing legislation. Such an approach could constrain the proliferation of LAWS – albeit within narrower confines than originally hoped for by many of the parties to the CCW – and is perhaps realistic.
II. Minimum Viable Product LAWS

The debate around LAWS is implicitly split between the exquisite capabilities under development by the US, China and other major powers, and less advanced systems that have been, or might be, developed by non-state actors, defence manufacturers or militaries with limited budgets. LAWS manufactured by responsible defence companies are typically designed to comply with the laws of armed conflict and are subject to rigorous testing before entering service – although this itself is technically demanding.\(^\text{34}\) This is less true of MVP LAWS that use non-military grade components – where the technical, intellectual and financial bar for entry is low – including commercial off-the-shelf and dual-use technology, open source software and even detailed instructions for how to build non-lethal capabilities, such as autonomous sentry paintball guns,\(^\text{35}\) or hobby drones adapted for more dangerous uses.\(^\text{36}\)

Individual MVP Use

The level of expertise for MVP LAWS need not be that high. Image-recognition-based targeting capabilities can legitimately be developed for commercial purposes by individuals using open source software and commercial components. For example, individuals have created ‘smart cat flaps’ for their homes using image recognition software that detects when cats are carrying prey and keeps the cat flap locked.\(^\text{37}\) One used YOLO, an object recognition algorithm that classifies objects using training images, while another learned to code specifically for the purpose, indicating that no prior expertise is needed. It follows that suitably motivated combatants could adopt this dual-use image recognition

---

\(^{34}\) Sean Welsh, ‘Calls for Regulation of Autonomous Weapons Pose Coding Challenge’, Janes Intelligence Review, 17 June 2021.


\(^{36}\) Peter Dockrill, ‘First-Ever Drone Swarm Attack has Struck Russian Military Bases, Sources Claim’, ScienceAlert, 11 January 2018; Sam Crackne-Evans, ‘As Small Drones Shape How We Fight, is the British Army Ready to Face Them?’, RUSI Commentary, 21 July 2022.

technology for LAWS, for example using open source, pre-trained neural networks against an occupying force’s vehicles and personnel. For example, given the length of NATO’s deployment to Afghanistan, or the ongoing conflicts in Libya, Syria and Ukraine, which involve consistent terrain, vehicle types and uniforms, such forces would be vulnerable to relatively simple MVP LAWS. IS in Mosul, for example, would only need a program capable of recognising the M1A1 Abrams and T-72 tanks sold to Iraq – a relatively straightforward task when they were the only tanks in the city. Consequently, narrowly defined operational scenarios in which Western forces often find themselves could allow adversaries to deploy MVP LAWS against them using readily available autonomous target recognition and engagement.

The cat flaps mentioned above were developed using software already available from experts. This differentiates the risks of LAWS proliferation from other proliferation risks: nuclear scientists capable of building and developing a nuclear weapon are rarer than computer programmers, and the engineering challenge is significantly greater for nuclear capabilities. Already happening in Ukraine, it is reasonable to presume that in future conflicts there is scope for programmers to become involved and develop autonomous weapons or technologies based on experience gained in the commercial sector. This vector has precedent. In 1995, Japanese cult terrorist group Aum Shinrikyo released a sarin gas nerve agent on the Tokyo subway, killing 12 people and injuring 5,000 more.\(^{38}\) One member of the group, Masami Tsuchiya, held a Master’s degree in chemistry and developed a working sarin gas from library books and his university education. Increasing production of the gas led to a reduction in the product’s purity, but it was nonetheless capable of causing extensive harm when released.\(^{39}\) Aum Shinrikyo also funded and ran a biological weapons programme, which was less effective than its chemical weapons programme, but the group’s success in developing these weapons, while limited, demonstrates what can happen when those with the right knowledge turn their hand to nefarious activity. There are clear parallels with AI.

MVP LAWS, including commercially available civilian autonomous platforms, are accessible by individuals, non-state actors and states facing larger, more powerful armed forces. They are, however, fragile, and are likely to be the resort of weaker powers against stronger ones.


Armed Forces’ MVP Use

Since 2014, Ukraine has employed hobby drones against Russian forces in Donbas. The country’s armed forces were not prepared for the war and had been described as ‘an army literally in ruins’. Innovation occurred organically from the bottom up, with one unit converting a Saxon armoured vehicle into a drone control centre for conducting strikes on Russian positions. Over time, Ukrainian society responded to the threat, leading to innovations in software, for example, GIS Arta, which uses GPS and digital mapping to track the positions of Ukrainian artillery systems. When a target is detected, it is logged, almost in real time, and the system’s algorithms decide which artillery system is best placed to conduct an engagement. The human gun crew may not see or visually confirm the target. The GIS Arta’s autonomy appears to be limited to selecting the most suitable weapon, but it is relevant to debates about proliferation because it was developed by Ukrainian civilians and taken up by the armed forces without defence industry involvement.

Building on this, the company Saker developed an image recognition program to identify Russian armoured vehicles, including, according to the programmers, camouflaged vehicles. Saker claims its drones can self-correct after dropping a bomb to ensure that the next bomb is accurate. The program works, in part, because its operational scenario is narrow and the categories of potential targets are easily defined. It needs to identify Russian combat vehicles, a large but ultimately finite target set, aided by Ukraine operating many of the same platforms. It does not need to determine whether an identified tank is a T-72 or T-64, simply that it is a tank. As an operator directs the drone’s flight, the question of whether it is a Russian or Ukrainian tank is irrelevant. In limited deployment scenarios, therefore, MVP AI-assisted programs can identify and engage targets.

Some states – Iran in particular – have demonstrated a patient approach to the indigenous development of autonomous weapons, and are proactively proliferating them. However, the software and hardware are openly available and actors may

41. Author interview with Ukrainian veteran, Kyiv, October 2017.
be able to develop their own solutions if the will and need exist. In the case of non- or less-developed state actors, there may be an adoption advantage in embracing even relatively limited capabilities, so the MVP proliferation risk here is high. However, the essentially limited nature of MVP LAWS suggests that the impact of their use will generally be low in small-scale use. And non-state actors are unlikely to be able to procure, convert and prepare to use very large quantities of drones without creating a significant footprint. Non-state and state actors have used other technologies to attack on a small scale, including IEDs or human lone-wolf attacks, that have not had hugely destabilising effects. This does not, of course, preclude the impact on the public of the use of an MVP LAWS for a targeted assassination of a kind akin to Archduke Ferdinand’s assassination in June 1914, or an attack such as 9/11.
III. Military Off-the-Shelf LAWS

Where MVP LAWS are likely to be used by non-state actors and weaker militaries against stronger ones, they will be fragile and so standard militaries are more likely to prefer more capable MOTS LAWS. This proliferation avenue is, therefore, very likely, and probably will have greater impact. Dan Wasserbly argues that the development of such LAWS is more about will and ethical concerns than about the technology itself.\(^\text{45}\) This chapter focuses on what is an admittedly limited number of states with the ability to design and manufacture LAWS that could be exported to actual or potential opponents of Western militaries. Meaningful analysis of the proliferation risk presented by every nation and/or military is beyond the scope of this paper.

MOTS LAWS that can claim some form of autonomy fall into two broad categories: single-use weapons destroyed in engaging a target; and multiple-use systems that carry armaments for target engagement. The majority of those discussed here are aerial vehicles. Although developing underwater or surface vessels is, theoretically, straightforward, autonomous ground vehicles represent a greater challenge. The MOTS proliferation risk is largely dependent on the nature of the country that has developed the technology. Some have a legacy of proliferating destabilising and harmful technologies, others less so.

Multiple states are pursuing independent LAWS programmes. Indonesia operates an autonomous coastal surveillance system procured from Israel\(^\text{46}\) and has domestic companies examining other autonomous technologies.\(^\text{47}\) South Korea's Dodaam Systems received widespread condemnation in 2015 for its autonomous remote weapons station,\(^\text{48}\) while Hanwha has expressed the goal of automating its K9 self-propelled howitzer by 2040.\(^\text{49}\) The analysis in this chapter focuses on the potential for autonomous weapons to proliferate in ways that could bring


\(^{48}\) Benjamin Haas, “‘Killer Robots’: AI Experts Call for Boycott Over Lab at South Korea University’, The Guardian, 5 April 2018.

Western militaries into contact with them. So, while the countries below have a record of providing sensitive technologies to others, they are likely not alone in proliferating MOTS LAWS.

China

China represents a significant proliferation challenge. Beijing has assisted Pakistan in acquiring nuclear weapons, contributed to Iran's nuclear programme, and is critical in financing North Korea's regime. Publicly, China supports both prohibition and regulation of the use of LAWS, but this contradicts the private rhetoric of the People's Liberation Army and the Chinese Communist Party. China's expansive R&D budget and close links between its universities and defence industry mean dual-use technologies and new developments in autonomy may be easily absorbed into the development of LAWS.

China's defence industry is one of the few to have developed and sold LAWS on the international market. In 2018 it was reported that Ziyan had sold its Blowfish A2 drone to the United Arab Emirates (UAE), and by 2019 was in negotiations with Saudi Arabia and Pakistan for the same system. The Blowfish can form ad hoc swarms, and carries an AI-augmented targeting system allowing it to search for, identify and acquire targets, adjusting its aim and autonomously select the ‘trigger time’ to engage the target. The level of human involvement is unclear, although the Blowfish is understood to include some form of ground control station that allows an operator to halt a mission if required. When swarming, the Blowfish relies on a module that ‘is capable of autonomously performing formations, attack functions, and collision avoidance’. The operator selects the attack profile, suggesting the operator might select a target, which the Blowfish swarm then decides how to attack. This form of autonomy is replicated in other Chinese designs, as well as the UAE’s Hunter 2S.

In 2021, the China Electric Power Research Institute revealed its UAV swarm system for reconnaissance, electronic warfare, ‘information countermeasures’ and kinetic strikes – its name roughly translates as ‘Swarm No. 1 Marine Vehicle’.

---

55. Ibid.
It uses an off-road truck chassis to carry 48 loitering munitions in a launch rack with space in the cabin for the crew. The level of human involvement is not clear, but it appears that humans select the target, and the swarm decides its approach and tactics for the engagement.

**Iran**

Iran arguably represents the greatest proliferation risk, having provided weapons and expertise to the Houthis in Yemen.\(^{56}\) Iran’s Quds Force, part of the Islamic Revolutionary Guard Corps, has led and supported proxy forces since its establishment in 1979.\(^{57}\) This assistance includes the provision of arms and training, including ballistic missiles and kamikaze drones, that have enabled the Houthis to attack targets in Saudi Arabia.\(^{58}\) In February 2023, the UK presented evidence to the UN that Iran supplied advanced weapons to the Houthis in violation of a UN Council Resolution.\(^{59}\) In 2022, Hizbullah’s leader, Sayyed Hassan Nasrallah, indicated that his group could turn their arsenal of unguided rockets into guided missiles with the help of Iran.\(^{60}\) In August 2022, an attack was conducted on the US base at Al-Tanf in Syria by an Iran-backed militia using KAS-04 drones supplied by Iran.\(^{61}\) Most recently, Iran has transferred a large quantity of UAVs and loitering munitions such as the Shahed-136 to Russia, which have contributed to Russia’s war in Ukraine.\(^{62}\)

Iran intends to be an early adopter of LAWS, and has developed several drones reportedly capable of autonomously locating and engaging ground-based as well as airborne targets.\(^{63}\) Iran’s developments in LAWS technology may well follow the MVP paradigm, but at a state level. Iran’s willingness to distribute sensitive technologies to proxy forces and partners represents a significant proliferation risk.

---

Israel

While not a direct threat to Western armed forces, Israel presents a proliferation pathway as it has sold military systems to others who could use, transfer or re-engineer them. The Harpy is arguably the most successful LAWS by export sales – in service with Azerbaijan, China, India, Israel, South Korea and Turkey. In the 2000s, there were efforts to modify the Harpy so that it could autonomously locate and detect missile launchers before contacting the operator for strike authorisation. Subsequent developments from the Harpy’s manufacturer, IAI, have eschewed fully autonomous targeting – for example, the Harop requires human control at all times, but flies autonomously to the selected area. Similarly, Elbit, which manufactures the Lanius, a racing quadcopter design, has been explicit that ‘attack missions require man-in-the-loop control to approve fire procedures’. However, while this would not be easy, there is a risk that human-in-the-loop functions could be overridden by malicious actors with the requisite skills, or replicas made without this safety check – although replicas are likely to be more basic and potentially more easily countered.

Israel is also a leader in autonomous ground vehicles. The Carmel programme, launched in 2019, allows the crew to monitor the vehicle’s autonomous actions and interfere if necessary. The solution, based around IAI’s Athena software, can be installed on any platform and is designed to autonomously detect and categorise threats, navigate with or without pre-planned routes, and make decisions about whether or not to alert the operators to any detected threats. So, although not a weapon system, the technology could be combined with other elements to create a LAWS.

Israel’s attitudes to LAWS could be shaped by many factors, but a significant factor in Israel’s foreign relations is its reliance on the US, which in the past has exerted political pressure on Israel to cancel arms deals and research links with China, for example. Where Israeli exports of LAWS run counter to US interests, there will likely be political pressure to prevent those sales from occurring. The proliferation risk presented by Israel is, therefore, mixed. The country is arguably

68. Wasserbly, ‘AUSA 2021’.
69. Ibid.
the most capable of completing the development of LAWS and selling them to other users, but its delicate relations with the US will likely limit the potential spread of these technologies.

Russia

The Russian Lancet loitering munition allegedly has autonomous capabilities and has been deployed operationally in Ukraine and Syria. The level of automation is not clear.\textsuperscript{71} The manufacturer, Kalashnikov, claims it is ‘capable of autonomously finding and hitting a target’,\textsuperscript{72} but there is no firm evidence of its ability to conduct completely autonomous engagements.\textsuperscript{73} However, a captured Lancet was found to carry a Nvidia TX2 single-board computer, which is designed for the edge processing of video data.\textsuperscript{74} This suggests that the Lancet may be capable of AI-supported targeting and video tracking. The same technology may also be used for autonomous navigation through the use of terrain features. The Lancet has been used more than 900 times in Ukraine, but video footage frequently released from it indicates that it is manually guided onto a target.\textsuperscript{75}

Nonetheless, Russian manufacturers and thinkers have expressed the view that proliferation of autonomous platforms is inevitable, and that Russia will have to create its own technologies to remain competitive.\textsuperscript{76} The war in Ukraine will likely impact Russia’s perceptions in this area, although it is not clear how. Further development will be hindered by Western sanctions, as many of Russia’s most advanced weapons rely on Western-supplied microelectronics.\textsuperscript{77} While sanctions will not completely deny access to the chips required for Russian LAWS, this and the loss of Russian expertise will also limit their development and subsequent proliferation.\textsuperscript{78}

\textsuperscript{71} Brennan Deveraux, ‘Loitering Munitions in Ukraine and Beyond’, \textit{War on the Rocks}, 22 April 2022.
\textsuperscript{73} Gregory Allen, ‘Russia has Probably Not Used AI-Enabled Weapons in Ukraine, But That Could Change’, CSIS, 26 May 2022.
Turkey

The Kargu is a loitering munition that gained notoriety in 2021 after a UN report into arms embargo violations in Libya claimed it had been used to autonomously engage fleeing targets.\(^79\) The specifics of this claim have been disputed, and it is not clear how much autonomy the system is actually designed to employ.\(^80\) Less is said about STM’s Alpagu, which is described as an autonomous tactical attack UAV. A promotional video from 2017 claims that it has sophisticated computer vision and deep learning algorithms, however it also appears to show a human operator.\(^81\) This suggests that while parts of the targeting cycle are automated and augmented with AI, the weapon itself may not be fully autonomous.

Nonetheless, Turkey’s arms industry has a broad swathe of advanced capabilities, from high-energy lasers to electronic warfare and armed drones.\(^82\) It is increasingly exporting its capabilities, particularly autonomous capabilities.\(^83\) While a NATO ally, Turkey has been willing to ignore arms embargoes where it considers its strategic interests are at stake.\(^84\) Consequently, Turkey represents a proliferation risk because the proxy forces it has supported may not use the technology responsibly.\(^85\) Nonetheless, the country is subject to diplomatic pressure from the US and others, which can shape its actions.\(^86\)

---

82. Based on author’s experience in the defence media industry and from conversations at the IDEF 2019 defence exhibition in Istanbul.
The UAE

The UAE is pursuing autonomous capabilities and smart weapons through EDGE, a defence conglomerate of multiple national defence companies. In February 2022, EDGE subsidiary Halcon released initial details of its Hunter 2S swarming loitering munition concept, where the company’s CEO remarked on the level of autonomy. Details were scarce, but a Halcon promotional video shows a separate remotely piloted aircraft system conducting reconnaissance of a military installation before a human operator selects several targets. The launch vehicle fires multiple Hunter 2S munitions, which form a swarm. As the munitions approach the target destination, they share data on how to attack each of the selected targets, which includes the allocation of munitions to each target. In the terminal phase, the munitions separate and engage their respective targets as a coordinated swarm.

The UAE is a growing presence within the international arms sales market and EDGE is already ranked as one of the world’s largest arms exporters. The UAE and EDGE have made clear their intention to become market leaders in key technologies, including autonomous platforms, and to exploit AI-enabled technologies. This, combined with its existing presence on the international arms market, indicates that the UAE is a likely avenue for the proliferation of MOTS LAWS. However, as with Israel and Turkey, the UAE is likely to face pressure from the US and its regional neighbours to avoid selling sensitive technologies to users whose interests might run counter to those of the UAE’s allies and partners.

IV. Boutique LAWS

While non-state actors or states with smaller budgets might exploit LAWS, these are of lower cost and complexity and are thus likely to be, individually, of lower impact than the boutique systems being explored by the US, China and others. Boutique programmes typically focus on networked sensor integration and stealthy airframes, placing them beyond the reach of all but the richest and most determined nations.\(^91\) Russia aspires to such platforms, but sanctions since its invasion of Ukraine and the cost of rebuilding its forces may well prevent it from pursuing the technology,\(^92\) even if it is technically capable of doing so, which is uncertain.\(^93\) Russian munitions used in Ukraine indicate that Russia relies on Western microelectronics to enable the most basic functions of its advanced weapons, although it is working to wean itself off such dependence.\(^94\) Consequently, the likelihood of boutique autonomy proliferating is lower than for MVP or MOTS LAWS, because of the costs and industrial sophistication involved and the desire by those few nations involved to protect their more sensitive technologies. Should proliferation occur, the impact is significantly greater.

The US Air Force Skyborg Programme was established to explore varying degrees of autonomy in human–machine teams.\(^95\) Operating alongside Next Generation Air Dominance, it aims to develop next-generation combat air capabilities, including loyal wingman drones and new command-and-control systems.\(^96\) Others are also developing loyal wingman drones, including Airbus (in Europe),\(^97\) Turkey (Programme Kizilelma),\(^98\) Australia (Ghost Bat)\(^99\) and the UK. China has also joined the fray with its FH-97A, which is orientated towards aerial combat

---

93. Author online interview with computer scientist and AI expert Stuart Russell, 22 June 2022; author online interview with Samuel Bendett, research analyst with the Center for Naval Analyses, 7 June 2022.
and breaching enemy air defences.\textsuperscript{100} The loyal wingman concepts generally seek to unlock difficult missions for air forces such as augmenting aerial situational awareness in heavily defended airspace, or penetration and suppression of enemy air defences, which makes them potentially destabilising, albeit within very specific boundaries.

Creating systems designed to penetrate and defeat national defences could be destabilising, but this should not be overstated. Air defence networks are not perfect solutions and are vulnerable to strikes from the air, land and sea. However, it is possible that future iterations of these and other boutique autonomous weapons could lead to fractious international relations. An example might be the potential effects of autonomous weapons designed specifically to hunt and destroy elements of a country’s nuclear deterrent, such as the US Navy’s Sea Hunter, which is designed to conduct autonomous ocean patrols and track enemy submarines.\textsuperscript{101}

Concerns about the impact of boutique autonomy on stability focus on how these capabilities may affect strategic decision-making, including timescales and escalation dynamics. States facing each another with boutique LAWS might fear sudden attack, particularly against nuclear capabilities, compressing the timelines for strategic decision-making in an environment where AI is also amplifying disinformation and rhetoric.\textsuperscript{102} The US ‘Star Wars’ Strategic Defence Initiative, developed in the late 1980s, drove the Soviet Union to seek asymmetric technologies, such as anti-satellite and silo-defence weapons, and may have contributed to a deterioration in US–Soviet relations.\textsuperscript{103} This is the niche into which the kind of boutique autonomy sought by NATO states and China could fit, suggesting cause for concern about the proliferation of these systems if they were to lead to instability between global powers.

The picture is mixed. Boutique LAWS could create asymmetries of risk through a perception of a lower human cost of war, either encouraging more aggressive behaviour or creating misunderstanding about an opponent’s willingness to contest an issue. Conversely, boutique LAWS could give opposing powers the impression that Western forces are less willing to accept the costs of war escalation, or drive escalation risk, because of their target set. In either scenario,


the lack of information about the capabilities of boutique LAWS and their intended uses, as well as the impossibility of knowing what a potential enemy is thinking, suggest caution around development and signalling is warranted.

Weapons designed specifically to target an opponent’s nuclear deterrent – autonomous or otherwise – carry immense potential for destabilising the international order and endangering peace and security should one nation feel its nuclear capability can be defeated and thus is no longer a deterrent. This is realistically only within the reach of boutique autonomous technologies and the countries pursuing them. A similar situation may be found in ballistic missile defence capabilities – also technically difficult and within the reach of very few nations – where the destabilising effect on the nuclear balance was such that parties agreed to limit their anti-ballistic missile capabilities through treaties, although the political consensus broke down and the US withdrew from the Anti-Ballistic Missile Treaty in December 2001.104

Proliferation of boutique autonomy is not impossible, even if it is less likely than for MVP or MOTS. Proliferators will still have to prove that the LAWS on offer either augment existing capabilities or exceed them and enable fundamentally new types of operation, and that they can do this at a competitive price. And, having done that, they will need agreement from their governments, who are likely to wish to protect their highly sensitive technologies. The militaries adopting them are also subject to the innovation challenges discussed by Theo Farrell and David Kilcullen, which, these authors suggest, constrain the capacity for radical change under normal circumstances.105 It follows that their adoption and proliferation might be accelerated by the threat or outbreak of a major war, either demonstrating their utility or affecting one of the developer nations and pushing them to seek out autonomous solutions. Without some kind of catalyst, development and proliferation of acceptable solutions is likely to take another decade, with gradual increases in capability throughout that period leading up to truly autonomous weapons. Whether the war in Ukraine and US concerns over China’s intentions towards Taiwan are such a catalyst remains to be seen. Even if the technology advances more quickly, the proliferation of the systems themselves may be more limited, given the destabilising impact they pose and the desire of governments to protect the most sensitive technologies that give them an edge.

If political will and support for expensive programmes such as the Future Combat Air System and Skyborg are maintained, these systems will eventually enter

---

service. However, there is an extensive period of trials and evaluations that the programmes must successfully navigate before this will happen. Because of this, their limited proliferation is considered likely but more constrained than for MOTS products. Furthermore, boutique autonomy may prove very destabilising, depending on the way in which it is employed and the political messaging attached to it. It must be understood that these weapons will enable and inform political decisions, which are what may ultimately lead to war, rather than proliferate war themselves. They may, however, give rise to uncomfortable conversations and questions about a country’s intentions to act. And while traditional weapons can be used to do many of the same things, they are less novel and thus less psychologically threatening.
The mere existence of LAWS technology is not enough to drive proliferation, let alone amount to its effective fielding. At its highest levels, warfare is an immensely complex human event involving societal pressures that defy simple explanation. At the sharp end of a war, it is common for historians to focus on a specific technology, for example, tank warfare or strategic bombing during the Second World War. However, this form of analysis ignores, whether deliberately or unintentionally, the enormous complexity of militaries at war. LAWS, although not widely used in conflict, fall into a similar trap – easy to analyse based on their individual merits and to assess as a standalone weapon. It is more instructive to consider how they contribute to the totality of an armed force’s or non-state actor’s battlefield.

The circumstances that lend themselves to the development and proliferation of LAWS can be deduced, enabling assessments of the risks. For example, autonomous weapons designed to locate and engage air defence systems are technically possible and ethically straightforward; they target radar emissions of a certain frequency and nothing else. There are few civilian applications for these frequencies and so the risk of collateral damage is relatively low. The massed and concerted use of these weapons provides an almost immediate boost to the totality of an armed force’s battlefield, assuming that they can be integrated into the military system as a whole and are deployed at the right time and place. The cost–benefit–risk ratio favours these weapons, where the political will exists for their adoption, and the risk of instability is limited, as weapons with the same effect have been used for decades without disrupting the international order. The alternative is to risk expensive, and limited, fleets of aircraft and pilots, and other expensive assets, for example, stocks of ground-based long-range strike missiles, in defeating enemy air defences to achieve control of the air. And without control of the air, ground forces are very vulnerable, so the adoption advantage is clear.

In other cases, the benefits may be less obvious. Autonomous weapons that select their own targets using optical sensors and computer vision would only be as successful and survivable as the optical suite. Effective imaging systems, although commercially available, are typically very expensive. Furthermore, electro-optics can be disrupted by the use of smoke or camouflage, which in some cases can almost eliminate thermal emissions. Optics are also very vulnerable to

---

Assessing Autonomous Weapons as a Proliferation Risk
Paul O’Neill, Sam Cranny-Evans and Sarah Ashbridge

fragmentation and air-burst effects used in most conflicts, so, for autonomous ground vehicles at least, they could be damaged or degraded quickly without the manual fallback on which crewed armoured fighting vehicles can rely.\textsuperscript{107}

Even with object recognition improving and commercial investment making these technologies more widely available, acquiring the training data required for neural networks to account for all possible target sets the system might encounter is probably beyond the ability of small state or non-state actors, except in the most limited and permissive scenarios. Neural networks typically require large quantities of training data and computing power to improve their accuracy, which increases the training time.\textsuperscript{108} Furthermore, AI technologies, such as few-shot learning, are unlikely to overcome some uses of camouflage and deception.\textsuperscript{109} Finally, software and programming challenges are accompanied by significant hardware limitations. Complex LAWS need a degree of hardware complexity that is difficult to overcome without significant investment, which in turn leads to additional power requirements that can result in a weight–power spiral.\textsuperscript{110} This suggests that MVP and MOTS products are likely to be quite simplistic in nature and limited in their ability to conduct tasks requiring multiple calculations.

Adoption advantage requires these limitations to be weighed against what is already possible. Conventional indirect fires are devastating when combined with readily available and cheap drones,\textsuperscript{111} such as the DJI Mavic. The training burden is low enough that non-state actors can achieve these effects without having to invest in developing their own programmes.\textsuperscript{112} Russian forces in Ukraine have brought accurate artillery fire to bear within five minutes of identifying a target with a drone.\textsuperscript{113} This very rapid targeting procedure would be difficult to accelerate because it is limited by how quickly artillery can be loaded, the gun elevated and the round’s travel to the target. Automating the entire process is unlikely to improve the end result (rapid targeting time and precision) beyond the increased survivability conferred by the absence of crews.


\textsuperscript{111} David Hambling, ‘How Drones are Making Ukrainian Artillery Lethally Accurate’, \textit{Forbes}, 12 May 2022.


\textsuperscript{113} Jack Watling and Nick Reynolds, ‘Ukraine at War: Paving the Road from Survival to Victory’, RUSI, 4 July 2022, p. 7.
The massed swarm of autonomous drones, similar to the Hunter 2S, can have significant effects against opponents not prepared for the threat – reputedly IS employed 70 armed drones in a near-simultaneous attack on Iraqi forces in December 2016, halting Iraq's operations.\textsuperscript{114} Remotely operated drones are problematic militarily, but jamming the global navigation satellite system link or the operator's radio link can degrade and attrit them quickly, leading to high loss rates.\textsuperscript{115} Autonomy reduces or eliminates this vulnerability; the drones do not require command links to human operators, while alternatives to satellite navigation, such as an inertial or AI-based navigation, also increase resilience through preloaded coordinates and autonomous target selection. This is increasingly possible using commercial technology from the machine learning and computer vision market.\textsuperscript{116} US technology company Nvidia has produced a small nano-computer designed to run AI algorithms,\textsuperscript{117} while small-form computing and AI could reduce demands on space, weight and power within UAVs.\textsuperscript{118} Commercially available drones can also work as autonomous drone swarms.\textsuperscript{119} Autonomous technology could also enable VBIEDs or autonomous surface vessels designed to deliver payloads against ships, increasing an already challenging threat.\textsuperscript{120} This is theoretically possible using extant technology and will probably become more prevalent as interest in the technology grows. However, the damage from this type of simple LAWS would currently be quite indiscriminate, more like loitering munitions than truly autonomous weapons, and of limited impact. Ukraine's strikes against Russian ships and infrastructure using uncrewed aircraft and vessels have been of relatively limited military effect without mass or use in combination with other capabilities such as long-range missiles, although the political effect of individual strikes has been greater.

The ability to autonomously select a target within the ethical and legal constraints of the laws of armed conflict is problematic because machine learning creates problems that are difficult to answer. It is possible to know the data an algorithm has trained on, and how that might have impacted its decision-making, but in


\textsuperscript{115} Watling and Reynolds, ‘Ukraine at War’.

\textsuperscript{116} Author online interview with Gregory Allen, director, AI Governance Project, 22 July 2022.


\textsuperscript{120} The Ukrainian drone swarm launched against Russian naval vessels is indicative of the impact that autonomous technologies could have. See Luke Harding and Isobel Koshiw, ‘Russia’s Black Sea Flagship Damaged in Crimea Drone Attack, Video Suggests’, \textit{The Guardian}, 30 October 2022.
complex environments there are aspects of decision-making that the operator will not understand. Using humans to select targets in real time before releasing LAWS to engage could free forces to conduct other engagements simultaneously, imposing multiple dilemmas on an adversary. For artillery, it could enable ‘leader–follower’ operations, with some uncrewed howitzers in a battery, increasing mass without additional people. However, this is not a truly autonomous weapon according to most definitions. It is worth noting that this kind of technology would generate a swarming challenge that is difficult for today’s armed forces to face. Allowing LAWS to select their own targets introduces uncertainty and reduces the predictability of engagements, so confining automation to parts of the targeting cycle rather than the complete cycle could enhance battlefield outcomes, while limiting some of the potential risks.

Overall, the challenge to militaries from LAWS is currently manageable. However, LAWS change the approach to defeating enemy capabilities. Most weapons are designed to kill or disable the human operator or, for remotely operated systems, defeat the link between human and machine. Defeating LAWS, however, requires the ability to disable or destroy the platform, which is more difficult. It would require destructive capabilities, for example, man-portable air defence missiles, at all echelons, as well as some form of enhanced intelligence picture to communicate incoming threats quickly. This is expensive, even where relatively fragile MVP LAWS are being employed in mass, as the economic cost of destroying a single LAWS works against the defender.

LAWS proliferation depends on both the availability of the technology and the adoption advantage. For militaries, modern conventional weapons are very effective at delivering lethal effects when paired with modern software-based solutions, so the bar is high. It is likely, therefore, that autonomy will complement crewed capabilities in many cases. The adoption advantage bar is lower for weaker militaries and non-state actors, but MVP systems are often more fragile and thus more easily countered, although their use at scale poses its own challenges. Boutique systems are very capable, but their cost, complexity and instability potential suggest that their proliferation is less likely.
### Table 1: LAWS Proliferation Risk

<table>
<thead>
<tr>
<th>LAWS Type</th>
<th>User</th>
<th>Control</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Non-State</td>
<td>State</td>
<td>Proliferation</td>
</tr>
<tr>
<td>MVP</td>
<td>✓</td>
<td>✓</td>
<td>Difficult to control as the technology is readily and legitimately available and the knowledge required to harness civilian technologies to illicit purposes is widely available.</td>
</tr>
<tr>
<td>MOTS</td>
<td>✓</td>
<td>✓</td>
<td>Regulation possible at national and international levels. National regulation is through export controls and the like, but is likely to be patchy, with some actors exercising greater constraints than others. International controls are likely to be more uniform but harder to achieve.</td>
</tr>
<tr>
<td>Boutique</td>
<td>X</td>
<td>✓</td>
<td>Likely to be controlled by those states producing exquisite capabilities, because of the destabilising impact and requirement for sophisticated organisational structures and systems that are beyond the reach of many actors.</td>
</tr>
</tbody>
</table>

Source: Author generated.
Conclusion

Autonomous weapons are being used increasingly but are not a homogeneous capability: there are different capabilities with different proliferation and consequence risks. The changing policy framework reflects this; its dual-track approach combines regulation and prohibition, with a growing emphasis on regulation as a form of arms control.

Proliferation is a function of the technology’s availability and adoption advantage, which reflects the degree to which the technology provides an edge over a potential adversary. This depends on LAWS being:

- As effective as or better than humans and existing weapons in the same role, for example, suppression of enemy air defences or artillery fire.
- Cheaper than a human or existing weapon in the same role.
- Easy enough to develop and deploy so the opportunity costs of doing so do not outweigh any potential gain.

The adoption advantage varies depending on the type of LAWS and the nature of the adversary. This paper identifies three categories of LAWS:

1. **MVP**: These represent a very high proliferation risk, but the systems are currently fragile and less capable than many existing military capabilities. Adoption advantage for MVP LAWS favours criminal and non-state actors and weaker militaries. Stronger militaries need to be prepared to counter these kinds of LAWS, which, while they are unlikely to be hugely destabilising, could be used for isolated atrocities, for example 9/11-type events. Regulating access to MVP LAWS is likely to be impossible, as the knowledge and technology is too widespread, but shaping the environment for their use through clear statements of acceptability (normative control) and criminal law covering the use or sale of technology offers some opportunities.

2. **MOTS**: These are more robust and have a higher adoption advantage than MVPs, but they are still complex and require infrastructure and organisational capacity to exploit, so the proliferation risk into militaries and larger non-state actors is high. Many are still supervised systems rather than fully autonomous, but are more challenging to counter than MVPs. Currently, they complement but do not completely replace other conventional capabilities. Further proliferation should be expected, especially from countries or companies with more relaxed attitudes to arms control, and militaries need the ability to counter these systems. The war in Ukraine will accelerate proliferation, as relatively sophisticated weapons are captured and shared with those who
will copy them. As MOTS LAWS are largely, but not exclusively, in the hands of governments, some control is possible, including through existing mechanisms of international humanitarian law holding states to account for weapons use, but the problem of definitions still applies.

3. **Boutique**: These cost billions of dollars to develop and are difficult to operate, so are only in the hands of a few nations. While they are potentially the most destabilising type of LAWS, this results in their proliferation risk being relatively low, as there is an advantage in not allowing them to proliferate.

Governments – through, among others, their militaries, and police forces where LAWS are used by criminals – need to be able to respond to the risks posed by LAWS, either as users of such systems or because they will be the targets of them. Consequently, they have a vested interest in shaping the debate around LAWS. While an outright ban on all forms of LAWS is no longer practical, opportunities exist to deal with different types of LAWS differently. This will involve a combination of policy and capability choices, including creating space for debate in which the normative case for regulation can be made. This should be accompanied by strengthened criminal legislation dealing with LAWS use, and industrial requirement and export controls covering autonomous systems, and also semi-autonomous systems that could be developed to full autonomy through MVP enhancement. The risks also require the development of counter-LAWS capabilities, for example electronic warfare and integrated defences. As the threats are not just military, governments need information and capability sharing between military and civilian authorities, such as police and intelligence agencies. Ensuring that information-sharing mechanisms exist is crucial.

Currently, the LAWS debate is focused on ethics, legal definitions and boutique capabilities. There are numerous less capable but militarily potentially useful LAWS being developed that require further examination to understand the adoption advantage and risks because these weapons are likely to proliferate ahead of the exquisite capabilities sought by the world’s major powers.

The future is being written, but it has not been decided – militaries will have to play their part.
About the Authors

Paul O’Neill is a Senior Research Fellow in the Military Sciences team at RUSI. With over 30 years’ experience in the armed forces, his research interests cover national security strategy and the technological, organisational and people aspects of defence and security. He co-hosts the RUSI Talking Strategy podcast.¹²¹ He has degrees in Laws (Nottingham Trent University and the University of Leicester), Defence Studies (King’s College London) and International Relations (University of Cambridge).

Sam Cranny-Evans is an Associate Fellow at RUSI and a former RUSI Research Analyst in the Military Sciences team. Sam specialises in C4ISR, with a particular interest in AI, having worked for Helsing AI, and land warfare, having spent five years at the Janes Information Group. His research has included the development and modernisation of China’s People’s Liberation Army, artillery tactics in Ukraine and Russia’s concepts of escalation management. Sam has a degree in War Studies from the University of Kent.

Sarah Ashbridge is an Affiliate Expert at RUSI and a former Research Fellow in the Military Sciences team. Sarah’s academic background is in military history and forensic archaeology, with a special focus on the recovery of historical war dead, contemporary mortuary affairs and humanitarian law. Much of Sarah’s work concentrates on the ways in which climate change and sustainability affect defence, explored through the RUSI Greening Defence podcast.¹²² Sarah is a Deployable Team Member for Kenyon International Emergency Services and a proud volunteer with Operation Nightingale (Defence Infrastructure Organisation) and Breaking Ground Heritage.