# Don't **be** evil?

A survey of the tech sector's stance on lethal autonomous weapons

PAX

www.paxforpeace.nl

### Reprogramming War

This report is part of a PAX research project on the development of lethal autonomous weapons. These weapons, which would be able to kill people without any direct human involvement, are highly controversial. Many experts warn that they would violate fundamental legal and ethical principles and would be a destabilising threat to international peace and security.

In a series of four reports, PAX analyses which actors could potentially be involved in the development of these weapons. Each report looks at a different group of actors, namely states, the tech sector, universities & research institutes, and arms producers. The present report focuses on the tech sector. Its goal is to inform the ongoing debate with facts about current developments and to encourage technology companies to develop and publicize clear policies for where they draw the line between what they will and will not do in the space of military AI applications.

If you have any questions regarding this project, please contact Daan Kayser: kayser@paxforpeace.nl


### Colophon

August 2019
ISBN: 978-94-92487-44-5
NUR: 689
PAX/2019/12

Authors: Frank Slijper, Alice Beck, Daan Kayser and Maaike Beenes
Thanks to: Laura Nolan, Liz O'Sullivan, Toby Walsh, Marta Kosmyna, Mary Wareham and Michel Uiterwaal.
Cover illustration: 'Vector' by Kran Kanthawong
Graphic design: Het IJzeren Gordijn


### About PAX:

PAX works with committed citizens and partners to protect civilians against acts of war, to end armed violence and to build peace. PAX operates independently of political interests. PAX is a co-founder of the Campaign to Stop Killer Robots.


P.O. Box 19318
3501 DH Utrecht
The Netherlands

www.paxforpeace.nl
info@paxforpeace.nl




# Table of Contents

# Executive Summary

The development of lethal autonomous weapons has raised deep concerns and has triggered an international debate regarding the desirability of these weapons. Lethal autonomous weapons, popularly known as killer robots, would be able to select and attack individual targets without meaningful human control. This report analyses which tech companies could potentially be involved in the development of these weapons. It highlights areas of work that are relevant to the military and have potential for applications in lethal autonomous weapons, specifically in facilitating the autonomous selection and attacking of targets. Companies have been included in this report because of links to military projects and/or because the technology they develop could potentially be used in lethal autonomous weapons.

## Lethal autonomous weapons

Artificial intelligence (AI) has the potential to make many positive contributions to society. But in order to realize its potential, it is important to avoid the negative effects and backlashes from inappropriate use of AI. The use of AI by militaries in itself is not necessarily problematic, for example when used for autonomous take-off and landing, navigation or refueling. However the use of AI to allow weapon systems to autonomously select and attack targets is highly controversial. The development of these weapons would have an enormous effect on the way war is conducted. It has been called the third revolution in warfare, after gunpowder and the atomic bomb. Many experts warn that these weapons would violate fundamental legal and ethical principles and would destabilize international peace and security. In particular, delegating the decision over life and death to a machine is seen as deeply unethical.

## The autonomous weapons debate in the tech sector

In the past few years, there has been increasing debate within the tech sector about the impact of new technologies on our societies. Concerns related to privacy, human rights and other issues have been raised. The issue of weapon systems with increasing levels of autonomy, which could lead to the development of lethal autonomous weapons, has also led to discussions within the tech sector. For example, protests by Google employees regarding the Pentagon project Maven led to the company installing a policy committing to not design or deploy AI in "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people". Also more than 240 companies and organisations, and more than 3,200 individuals have signed a pledge to never develop, produce or use lethal autonomous weapon systems.

Tech companies have a social responsibility to ensure that the rapid developments in artificial intelligence are used for the benefit of humankind. It is also in a company's own interest to ensure it does not contribute to the development of these weapons as this could lead to severe reputational damage. As Google Cloud CEO Diane Green said, "Google would not choose to pursue Maven today because the backlash has been terrible for the company".



## The tech sector and increasingly autonomous weapons

A number of technologies can be relevant in the development of lethal autonomous weapons. Companies working on these technologies need to be aware of that potential in their technology and they need to have policies that make explicit how and where they draw the line regarding the military application of their technologies. The report looks at tech companies from the following perspectives:

- Big tech
- AI software and system integration
- Autonomous (swarming) aerial systems
- Hardware
- Pattern recognition
- Ground robots

## Level of concern

Fifty companies from 12 countries, all working on one or more of the technologies mentioned above, were selected and asked to participate in a short survey, asking them about their current activities and policies in the context of lethal autonomous weapons. Based on this survey and our own research PAX has ranked these companies based on three criteria:

1. Is the company developing technology that could be relevant in the context of lethal autonomous weapons?
2. Does the company work on relevant military projects?
3. Has the company committed to not contribute to the development of lethal autonomous weapons?

Based on these criteria, seven companies are classified as showing 'best practice', 22 as companies of 'medium concern', and 21 as 'high concern'. To be ranked as 'best practice' a company must have clearly committed to ensuring its technology will not be used to develop or produce autonomous weapons. Companies are ranked as high concern if they develop relevant technology, work on military projects and have not yet committed to not contributing to the development or production of these weapons.

## Recommendations

This is an important debate. Tech companies need to decide what they will and will not do when it comes to military applications of artificial intelligence. There are a number of steps that tech companies can take to prevent their products from contributing to the development and production of lethal autonomous weapons.

- Commit publicly to not contribute to the development of lethal autonomous weapons.
- Establish a clear policy stating that the company will not contribute to the development or production of lethal autonomous weapon systems.
- Ensure employees are well informed about what they work on and allow open discussions on any related concerns.

## Table:
COMPANIES SURVEYED FOR THIS REPORT

Companies have been ranked by levels of concern. The ranking was based on three criteria:

1. Is the company developing technology that could be relevant in the context of lethal autonomous weapons?
2. Does the company work on relevant military projects?
3. Has the company committed to not contribute to the development of lethal autonomous weapons?

| COMPANY | BEST PRACTICE | MEDIUM CONCERN | HIGH CONCERN | HQ | RELEVANT TECHNOLOGY | RELEVANT MILITARY/ SECURITY PROJECTS | COMMIT TO NOT DEVELOP |
|---|---|---|---|---|---|---|---|
| **AerialX** | | | ■ | Canada | Counter-drone systems | DroneBullet | |
| **Airobotics** | | ■ | | Israel | Autonomous drones | Border security patrol bots | |
| **Airspace Systems** | | | ■ | US | Counter-drone systems | Airspace interceptor | |
| **Alibaba** | | ■ | | China | AI chips, Facial recognition | - | |
| **Amazon** | | | ■ | US | Cloud, Drones, Facial and speech recognition | JEDI, Rekognition | |
| **Anduril Industries** | | | ■ | US | AI platforms | Project Maven, Lattice | |
| **Animal Dynamics** | ■ | | | UK | Autonomous drones | Skeeter | X |
| **Apple** | | ■ | | US | Computers, Facial and speech recognition | - | |
| **Arbe robotics** | ■ | | | Israel | Autonomous vehicles | - | X |
| **ATOS** | | ■ | | France | AI architecture, cyber security, data management | - | |
| **Baidu** | | ■ | | China | Deep learning, Pattern recognition | - | |
| **Blue Bear Systems** | | | ■ | UK | Unmanned maritime and aerial systems | Project Mosquito/LANCA | |
| **Cambricon** | | ■ | | China | AI chips | - | |
| **Citadel Defense** | | | ■ | US | Counter-drone systems | Titan | |
| **Clarifai** | | | ■ | US | Facial recognition | Project Maven | |
| **Cloudwalk Technology** | | ■ | | China | Facial recognition | - | |
| **Corenova Technologies** | | | ■ | US | Autonomous swarming systems | HiveDefense, OFFSET | |
| **DeepGlint** | | ■ | | China | Facial recognition | - | |
| **Dibotics** | | ■ | | France | Autonomous navigation, Drones | 'Generate' | |
| **EarthCube** | | | ■ | France | Machine learning | 'algorithmic warfare tools of the future' | |
| **Facebook** | | ■ | | US | Social media, Pattern recognition, Virtual Reality | - | |
| **General Robotics** | ■ | | | Israel | Ground robots | Dogo | X |
| **Google** | ■ | | | US | AI architecture, Social media, Facial recognition | - | X |
| **Heron Systems** | | | ■ | US | AI software, ML, Drone applications | 'solutions to support tomorrow's military aircraft' | |
| **HiveMapper** | ■ | | | US | Pattern recognition, Mapping | HiveMapper app | X |
| **IBM** | | ■ | | US | AI chips, Cloud, Super computers, Facial recognition | Nuclear testing super computers, ex-JEDI | |
| **Innoviz** | | ■ | | Israel | Autonomous vehicles | - | |
| **Intel** | | | ■ | US | AI chips, UAS | DARPA HIVE | |
| **Megvii** | | ■ | | China | Facial recognition | - | |
| **Microsoft** | | | ■ | US | Cloud, Facial recognition | HoloLens, JEDI | |
| **Montvieux** | | | ■ | UK | Data analysis, Deep learning | 'Revolutionise human information relationship for defence' | |
| **Naver** | | ■ | | S. Korea | 'Ambient Intelligence', Autonomous robots, Machine vision systems | - | |
| **Neurala** | | ■ | | US | Deep learning neural network software | Target identification software for military drones | |
| **Oracle** | | | ■ | US | Cloud, AI infrastructure, Big data | ex-JEDI | |
| **Orbital Insight** | | ■ | | US | Geospatial analytics | - | |
| **Palantir** | | | ■ | US | Data analytics | DCGS-A | |
| **Percepto** | | ■ | | Israel | Autonomous drones | - | |
| **Roboteam** | | | ■ | Israel | Unmanned systems; AI software | Semi-autonomous military UGVs | |
| **Samsung** | | ■ | | S. Korea | Computers and AI platforms | - | |
| **SenseTime** | | | ■ | China | Computer vision, Deep learning | SenseFace, SenseTotem for police use | |
| **Shield AI** | | | ■ | US | Autonomous (swarming) drones | Nova | |
| **Siemens** | | ■ | | Germany | AI, Automation | KRNS, TRADES | |
| **Softbank** | ■ | | | Japan | Telecom, Robotics | - | X |
| **SparkCognition** | | | ■ | US | AI systems, Swarm technology | 'works across the defense and national security space in the U.S.' | |
| **Synesis** | | | ■ | Belarus | AI- and Cloud-based applications, Pattern recognition | Kipod | |
| **Taiwan Semiconductor** | | ■ | | Taiwan | AI chips | - | |
| **Tencent** | | ■ | | China | AI applications, Cloud, ML, Pattern recognition | - | |
| **Tharsus** | | ■ | | UK | Robotics | - | |
| **VisionLabs** | ■ | | | Russia | Visual recognition | - | X |
| **Yitu** | | | ■ | China | Facial recognition | Police use | |

■ **HIGH CONCERN** Company working on military/security applications of relevant technologies + chose not to answer our survey's questions in a meaningful way.

■ **MEDIUM CONCERN** Company working on military/security applications of relevant technologies + answered that it was not working on lethal autonomous weapons; or Company not known as working on military/security applications of relevant technologies + chose not to answer our survey's questions in a meaningful way.

■ **BEST PRACTICE** Company answered to explain its policy on how it ensures its technology is not contributing to lethal autonomous weapons.

\- Unknown.

**NB:** This table ranks companies according to the level of concern regarding their potential (unintended) contribution to the development of lethal autonomous weapons. It does not take into account other concerns regarding privacy, human rights and other issues.

# 1. Introduction

Artificial Intelligence (AI) is progressing rapidly and has enormous potential for helping humanity in countless ways, from improving healthcare to lifting people out of poverty, and helping achieve the United Nations Sustainable Development Goals – if deployed wisely.[1] In recent years, there has been increasing debate within the tech sector about the impact of AI on our societies, and where to draw the line between acceptable and unacceptable uses. Concerns related to privacy, human rights and other issues have been raised. The issue of weapon systems with increasing levels of autonomy, which could lead to lethal autonomous weapons, has also led to strong discussions within the tech sector.

In reaction to a project with the Pentagon, Google staff signed an open letter saying "We believe that Google should not be in the business of war".[2] Following the controversy Google published its AI principles, "which include a commitment to not pursue AI applications for weapons".[3]

Microsoft employees responded to the company's efforts to participate in another US military contract by affirming that they worked at Microsoft in the hope of empowering "every person on the planet to achieve more, not with the intent of ending lives and enhancing lethality".[4]

In 2014, Canadian company Clearpath Robotics was the first company committing not to contribute to the development of lethal autonomous weapons. It said: "This technology has the potential to kill indiscriminately and to proliferate rapidly; early prototypes already exist. Despite our continued involvement with Canadian and international military research and development, Clearpath Robotics believes that the development of killer robots is unwise, unethical, and should be banned on an international scale".[5]

In order to realize the great above-mentioned potential for AI to make the world better, it is important to avoid the negative effects and backlashes from inappropriate AI use. The use of AI by militaries is not necessarily problematic, for example for autonomous take-off and landing, navigation or refueling. However, the development of lethal autonomous weapons, which could select and attack targets on their own, has raised deep concerns and triggered heated controversy.

This is an important debate in which tech companies play a key role. To ensure that this debate is as fact-based and productive as possible, it is valuable for tech companies to articulate and publicise clear policies on their stance, clarifying where they draw the line between what AI technology they will and will not develop.

## Concerns about Lethal Autonomous Weapons

Lethal autonomous weapon systems are weapons that can select and attack individual targets without meaningful human control.[6] This means that the decision to use lethal force is delegated to a machine, and that an algorithm can decide to kill humans. The function of autonomously selecting and attacking targets could be applied to various autonomous platforms, for instance drones, tanks, fighter jets or ships. The development of such weapons would have an enormous effect on the way war is conducted and has been called the third revolution in warfare, after gunpowder and the atomic bomb.[7]

Many experts warn that lethal autonomous weapons would violate fundamental legal and ethical principles and would be a destabilising threat to international peace and security. Moral and ethical concerns have centred around the delegation of the kill decision to an algorithm. Legal concerns are related to whether lethal autonomous weapons could comply with international humanitarian law (IHL, also known as the law of war), more specifically whether they could properly distinguish between civilians and combatants and make proportionality assessments.[8] Military and legal scholars have pointed out an accountability vacuum regarding who would be held responsible in the case of an unlawful act.[9]

Others have voiced concerns that lethal autonomous weapons would be seriously destabilizing and threaten international peace and security. For example, by enabling risk-free and untraceable attacks they could lower the threshold to war and weaken norms regulating the use of force. Delegating decisions to algorithms could result in the pace of combat exceeding human response time, creating the danger of rapid conflict escalation. Lethal autonomous weapons might trigger a global arms race where they will become mass-produced, cheap and ubiquitous since, unlike nuclear weapons, they require no hard-to-obtain raw materials. They might therefore proliferate to a large number of states and end up in the hands of criminals, terrorists and warlords. Sized and priced smartphones, lethal drones with GPS and facial recognition might enable anonymous political murder, ethnic cleansing or acts that even loyal soldiers would refuse to carry out. Algorithms might target specific groups based on sensor data such as perceived age, gender, ethnicity, dress code, or even place of residence or worship. Experts also warn that "the perception of a race will prompt everyone to rush to deploy unsafe AI systems".[10]

"Because they do not require individual human supervision, autonomous weapons are potentially scalable weapons of mass destruction; an essentially unlimited number of such weapons can be launched by a small number of people. This is an inescapable logical consequence of autonomy", wrote Stuart Russell, computer science professor at the University of California in Berkeley.[11] Therefore, "pursuing the development of lethal autonomous weapons would drastically reduce international, national, local, and personal security".[12] Decades ago, scientists used a similar argument to convince presidents Lyndon Johnson and Richard Nixon to renounce the US biological weapons programme and ultimately bring about the Biological Weapons Convention.

Twenty eight states, including Austria, Brazil, China, Egypt, Mexico and Pakistan, have so far called for a ban, and most states agree that some form of human control over weapon systems and the use of force is required.[13] UN Secretary-General António Guterres has called lethal autonomous weapons "morally repugnant and politically unacceptable", urging states to negotiate a ban on these weapons. The International Committee of the Red Cross (ICRC) has called on states to establish internationally agreed limits on autonomy in weapon systems that address legal, ethical and humanitarian concerns. The Campaign to Stop Killer Robots, a coalition of over a hundred civil society organisations across 54 countries, aims to stop the development and use of fully autonomous weapons through an international treaty. An IPSOS poll in 26 countries shows that 61 per cent of respondents oppose lethal autonomous weapons. Two-thirds answered that such weapons would "cross a moral line because machines should not be allowed to kill".[14]

## This Report

This report analyses developments in the tech sector, pointing to areas of work that are highly relevant to the military and have potential for applications in lethal autonomous weapons, specifically in facilitating the autonomous selection and attack of targets. While certain technologies may well ensure sufficient human control over a weapon's use, it is often unclear what this entails and how this is ensured. Similarly, certain technologies may be intended for uncontroversial uses that do not cause harm, but it is often unclear how companies ensure their technology will not be used for lethal applications, and especially not for autonomous weapons.

Whereas military production in the past was naturally the domain of the arms industry, with the emergence of the digital era, the tech sector has become increasingly involved. Thus this report analyses the connections between the public and private sectors in the area of military technology with increasingly autonomous capabilities.

The research is based on information available in the public domain, either from company websites or from trusted media. PAX also sent out a survey to 50 companies in the tech sector that we deemed relevant because of their (actual or potential) connections with the military, as a development partner and/or as a supplier of specific products. The survey asked companies about their awareness of the debate around autonomous weapons, whether the company has an official position regarding these weapons, and whether they have a policy to reflect this position (See 'Annex: Survey Questions'). These companies have been ranked based on three criteria

1. Is the company developing technology that could be relevant in the context of lethal autonomous weapons?
2. Does the company work on relevant military projects?
3. Has the company committed to not contribute to the development of lethal autonomous weapons?

It is important to note that companies mentioned in this report have been included because of links to military projects and/or because the technology they develop could potentially be used in autonomous weapons. A natural assumption is that companies are not contributing to the development of lethal autonomous weapons if they responded to our survey stating that they do not work on this and have a policy to prevent such use. It is valuable for the ongoing debate that tech companies, regardless of their stance, articulate it into a clear policy that is publicly shared.

This report is not intended to be an exhaustive overview of such activities, nor of the tech sector itself; rather, it covers a relevant range of products and companies to illustrate the role of this sector in the development of increasingly autonomous weapons. This role brings a responsibility for tech companies to be mindful of the potential applications of certain technologies and possible negative effects when applied to weapon systems.



Many emerging technologies are dual-use and have clear peaceful uses. In the context of this report, the concern is with products that could potentially also be used in lethal autonomous weapons. Moreover, there is the worry that unless companies develop proper policies, some technologies not intended for battlefield use may ultimately end up being used in weapon systems.

The development of lethal autonomous weapons takes place in a wide spectrum, with levels of technology varying from simple automation to full autonomy, and being applied in different weapon systems' functionalities. This has raised concerns of a slippery slope where the human role is gradually diminishing in the decision-making loop regarding the use of force, prompting suggestions that companies, through their research and production, must help guarantee meaningful human control over decisions to use force.

In the hope of contributing to the discussion, this report illustrates some developments in this area, with varying levels of (proclaimed) autonomy or use of AI. The information in the report is based on publicly available information. However, not all technical information about companies' technologies and projects is publicly available. Therefore, the report does not draw conclusions from the perceived levels of autonomy and human control in the products and projects described in the report.

# 2. The Autonomous Weapons Debate in the Tech Sector

In recent years, there has been increasing debate about the impact of AI on society. Concerns related to privacy, human rights and other issues have been raised. The issue of weapon systems with increasing levels of autonomy, which could lead to the development of lethal autonomous weapons, is an active area of discussion within the technology sector. Companies must decide whether or not they will participate in their development. As there are no multinational treaties or norms banning autonomous weapons yet, "professional codes of ethics should also disallow the development of machines that can decide to kill a human", according to professor Stuart Russell.[15]

## Tech against Lethal Autonomous Weapons

The first company to speak out on this issue was Clearpath Robotics in 2014. Co-founder Ryan Gariepy stated in an open letter that the company pledged not to "manufacture weaponized robots that remove humans from the loop".[16] While not objecting to military work per se, he stressed:

> *"As a company which continues to develop robots for various militaries worldwide, Clearpath Robotics has more to lose than others might by advocating entire avenues of research be closed off. Nevertheless, we call on anyone who has the potential to influence public policy to stop the development of killer robots before it's too late. We encourage those who might see business opportunities in this technology to seek other ways to apply their skills and resources for the betterment of humankind. Finally, we ask everyone to consider the many ways in which this technology would change the face of war for the worse. Voice your opinion and take a stance".*[17]

Since then, many more have added their voice to underline the risks of autonomous weapons. Since its publication in 2015, over 4,500 artificial intelligence and robotics experts, and more than 26,000 others signed an open letter stating:

> *"The key question for humanity today is whether to start a global AI arms race or to prevent it from starting. If any major military power pushes ahead with AI weapon development, a global arms race is virtually inevitable, and the endpoint of this technological trajectory is obvious: autonomous weapons will become the Kalashnikovs of tomorrow. […] We therefore believe that a military AI arms race would not be beneficial for humanity. There are many ways in which AI can make battlefields safer for humans, especially civilians, without creating new tools for killing people".*

The letter adds:

> *"Just as most chemists and biologists have no interest in building chemical or biological weapons, most AI researchers have no interest in building AI weapons — and do not want others to tarnish their field by doing so, potentially creating a major public backlash against AI that curtails its future societal benefits. Indeed, chemists and biologists have broadly supported international agreements that have successfully prohibited chemical and biological weapons, just as most physicists supported the treaties banning space-based nuclear weapons and blinding laser weapons".*[18]

Signatories include Elon Musk (CEO, Tesla and SpaceX), Eric Horvitz (managing director, Microsoft Research), Barbara Grosz (Harvard University), Demis Hassabis and Mustafa Suleyman (co-founders Google DeepMind), Yann LeCun (Vice President, Chief AI Scientist at Facebook), Professor Francesca Rossi (Padova University and Harvard), Steve Wozniak (co-founder Apple) and Kathryn McElroy (IBM's Watson design lead).

In 2017, 116 tech sector CEOs warned against these weapons and called on the United Nations to take action. "These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways. We do not have long to act. Once this Pandora's box is opened, it will be hard to close".[19] Yoshua Bengio, computer science professor at the University of Montreal, said on the occasion: "The use of AI in autonomous weapons hurts my sense of ethics" and that the development of autonomous weapons "would be likely to lead to a very dangerous escalation" and "would hurt the further development of AI's good applications".[20] Bengio, along with Yann LeCun and Geoffrey Hinton, received the 2018 A.M. Turing Award, also referred to as the Nobel Prize of Computing.[21]

Since 2018, over 240 companies and organisations, and over 3,200 individuals have signed a pledge to never develop, produce or use lethal autonomous weapon systems.

> *"Thousands of AI researchers agree that by removing the risk, attributability, and difficulty of taking human lives, lethal autonomous weapons could become powerful instruments of violence and oppression, especially when linked to surveillance and data systems. […]*
>
> *We, the undersigned, call upon governments and government leaders to create a future with strong international norms, regulations and laws against lethal autonomous weapons. These currently being absent, we opt to hold ourselves to a high standard: we will neither participate in nor support the development, manufacture, trade, or use of lethal autonomous weapons. We ask that technology companies and organizations, as well as leaders, policymakers, and other individuals, join us in this pledge".*[22]

Companies that signed include Google's DeepMind, Clearpath Robotics and Silicon Valley Robotics.

Furthermore, in 2019 the Federation of German Industries (BDI) released a position paper calling for a ban on lethal autonomous weapon systems.

> *"The impact of artificial intelligence on security and defence cannot be overstated. There are significant ethical reservations about the opportunities for faster and more accurate applications. The BDI calls for a ban on lethal autonomous weapon systems and is committed to an international regulatory framework".*[23]

## Tech Workers

There have been debates within tech companies themselves too, highlighting the growing activism and social engagement of tech workers. They have been voicing their concerns about the applications of the technologies they are working on. Tech workers are increasingly demanding clarity and transparency on the intended applications of the technologies they develop, stemming from a commitment to develop technology to help humanity and not to harm it.

Related to the use of artificial intelligence in weapon systems, the most notable example is that of **Google**. In 2018 thousands of Google staff signed an open letter that called on Google to cancel its collaboration with the Pentagon on Project Maven.[24]

The project uses artificial intelligence to interpret video images, which could provide the basis for automatic targeting and autonomous weapon systems.[25] "We believe that Google should not be in the business of war", the open letter stated.[26] Amr Gaber, one of the authors of the letter, said at the UN in 2018: "A program should never authorize an action to end the life of a human being".[27] Following the staff's letter, Google decided to not renew its contract and has since published ethical AI principles, which state that Google will not design or deploy AI in "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people".[28] Google reiterated that position in response to our survey request, further outlining that "since announcing our AI principles, we've established a formal review structure to assess new projects, products and deals. We've conducted more than 100 reviews so far, assessing the scale, severity, and likelihood of best- and worst-case scenarios for each product and deal".[29]

Another example is **Clarifai**, a company that works on machine learning and image recognition, and that is also involved in Project Maven. Its work on this project was initially very secretive. Reportedly, paper covered the windows of the room where the work took place and employees called it "The Chamber of Secrets", in reference to the Harry Potter novel. Even the eight engineers and researchers working inside the room did not entirely realize the nature of the project, according to "three people with knowledge of the matter", who spoke to the New York Times "on the condition that they not be identified for fear of retaliation".[30]

Despite the CEO's assurance that employees knew what they were working on, those employees were in fact not entirely clear about what it was specifically going to be used for, especially as the technology was "the same that they had been working on for other projects".[31] In a blogpost, CEO Matthew Zeiler wrote that "Clarifai's mission is to accelerate the progress of humanity with continually improving AI. After careful consideration, we determined that the goal of our contribution to Project Maven—to save the lives of soldiers and civilians alike—is unequivocally aligned with our mission". He added: "We believe in putting our resources toward society's best



"Project Maven's AI-driven identification of objects could quickly blur or move into AI-driven identification of "targets" as a basis for the use of lethal force."

Campaign to Stop Killer Robots

interests, and that includes America's security".[32] A week after the blog, Zeiler spoke at a staff meeting. "He did say that our technology was likely to be used for weapons," says Liz O'Sullivan, who has since left the company, "and autonomous weapons at that".[33] Zeiler has not denied this and has said that the US needs to step up, as other countries, including China, are already doing so.[34] In late 2018, Clarifai also announced the formation of a subsidiary called Neural Net One, which will deal with military and intelligence contracts.[35]

Despite this work, Clarifai opted not to take part in our survey, stating: "Given that autonomous weapons are not the company's focus, we won't be able to help with the survey".[36] This answer raises an important point. Even if a company itself does not focus on the development of weapon systems, its technology could very well be used for that purpose. Therefore it is crucial that companies such as Clarifai set up clear policies to make explicit what purposes their technology may be used for and what their clear red lines are. Without such policies, companies risk contributing to the development of lethal autonomous weapons.

Within **Microsoft**, there have also been debates about cooperation with the military. One example is the Joint Enterprise Defense Infrastructure (JEDI) programme. Various big tech companies have been bidding for this contract, including Microsoft, Amazon, Oracle and IBM, with the first two as the last remaining contenders.[37] JEDI is a USD 10 billion project to build cloud services for the US Department of Defense. Their Chief Management Officer John Gibson explained that "This program is truly about increasing the lethality of our department".[38] In an open letter, employees then countered that "many Microsoft employees don't believe what we build should be used for waging war", adding that they worked at Microsoft in the hope of empowering "every person on the planet to achieve more, not with the intent of ending lives and enhancing lethality".[39]

There was also opposition surrounding Microsoft's HoloLens contract with the Pentagon. The USD 479 million contract "could eventually provide more than 100,000 headsets designed for combat and training in the military". The Pentagon has described the project as a way to "increase lethality by enhancing the ability to detect, decide and engage before the enemy".[40] Once again, employees wrote a letter to Microsoft's CEO and President stating that the employees working on the lens believed "it would be used to help architects and engineers build buildings and cars, to help teach people how to perform surgery or play the piano, to push the boundaries of gaming. […] While

Liz O'Sullivan left Clarifai in 2018. She shared her views on autonomous weapons for this report.

"As technology today is increasingly owned by a concentrated few large companies, conscientious objectors have fewer options in terms of workplaces where they can be free from participating in acts of war. Even seemingly innocuous tools like an AR headset meant for gaming (Microsoft Hololens) can be repurposed into a tool meant to "increase lethality" on the battlefield.

Technology companies must take special care with the psychological safety of the people who build their tools. It is unrealistic to ask that technology companies never work with the military, and our soldiers do deserve the best technology to protect their lives. But special care must be paid to "dual use" technologies and the workers who build them. No worker should be forced to contribute to end a human life, doubly so without that worker's knowledge and consent, and yet this is the scenario faced by thousands of people across most of the major technology companies today.

With special attention to AI, and more specifically, computer vision tools that make use of "object detection" or "object localisation" (among other technologies), companies and workers alike must be aware of the potential impact this technology will have on the development of lethal autonomous weapons. This domain represents the last piece of the puzzle in killer robot development, and as such, any research that improves the state of the art for a military will enhance their attempts to further killer robot designs and efficacy.

Technology companies should take steps to ensure full and complete transparency with the workers who build dual use technologies, especially in any case where this product can be sold to the military for any purpose at all. They should include legal protections for workers who refuse to participate in building ethically murky projects, especially those that may aid in ending human lives. In the event that a company is offered a military contract for a dual use technology such as object localisation, they should either refuse, or take great care to ensure that the algorithms sold cannot be repurposed or used to any end other than the innocent use it is intended to perform. The latter option, of course, may not be enough to guarantee that this work will not somehow end up on the drawing board for the killer robot architect, and as such should be approached very delicately, with strong contractual stipulations and auditing as mandatory conditions.

Tech companies bear a lot of responsibility and power in the international landscape by the very nature of the projects they decide to take on. But, in the event that tech company leadership chooses money over peace, then the tech workers themselves have a rare opportunity to use their collective power to pressure these leaders into preventing the misuse of AI technologies for the purposes of escalating international tensions, or of ending human lives".

[Microsoft] has previously licensed tech to the US Military, it has never crossed the line into weapons development. [...] The application of HoloLens within the IVAS [Integrated Visual Augmentation System] system is designed to help people kill".[41] Microsoft has an ethics review committee called Aether, but employees say it is "not robust enough to prevent weapons development, as the IVAS contract demonstrates".[42] The letter calls on Microsoft to end the IVAS contract, to cease developing weapon technologies and draft a public-facing acceptable use policy clarifying these commitments, as well as to appoint an external ethics review board with the power to enforce and publicly validate compliance with the acceptable use policy.[43]

Responding to the survey, Eric Horvitz, director of Microsoft Research and chair of the Aether committee, mentions that "Microsoft makes a priority of the responsible development and use of AI technologies. Microsoft's cross-company Aether committee takes sensitive uses of AI technologies very seriously and deliberates carefully in making recommendations to our company's leadership team about controls and guidelines, including the critical need for human oversight and human-in-the loop on high-stakes, sensitive AI technologies."[44] Unfortunately his statement can not be considered the company's official position on lethal autonomous weapons.

In October 2018 Brad Smith, Microsoft's President, said the company would continue to sell software to the US military. He wrote: "We believe in the strong defense of the United States and we want the people who defend it to have access to the nation's best technology, including from Microsoft".[45] While military contracts are indeed not necessarily problematic, there are serious concerns when these technologies are used for lethal applications.

Whereas Smith has called for a Digital Geneva Convention, stating the need for "international rules to protect the public from nation state threats in cyberspace",[46] it is remarkable that one of the largest IT companies in the world has so far not announced any policy regarding lethal autonomous weapons. Taken together, this raises questions about Microsoft's position in potentially contributing to the development of autonomous weapons.

## AUTOMATING SIGNATURE STRIKES

Laura Nolan, a senior software engineer, left Google in June 2018 over the company's (then) involvement in Project Maven. She shared her ideas on autonomous weapons for this report:

"Autonomous weapon systems are dangerous. I've worked with software systems for years and no complex system I've ever worked with has been free of errors, often very serious ones. In a warfare context, this could cost lives, potentially many lives.

But an even greater consideration than the simple risk of autonomous weapon systems making attacks in violation of international humanitarian law is the problem of centralisation of power. It takes very few people to control a robot or drone army. Autonomous weapon systems become a new weapon of mass destruction, weakening the checks and balances we expect in the exercise of military power.

I left Google because the company was involved in developing Project Maven, a system that was intended to find objects (such as people and vehicles) in drone surveillance video. A system that can identify and track people over time can easily be programmed to find groups of certain sizes, or to look for other patterns of activity - this is a huge step towards automating signature strikes, attacks on targeted individuals or groups whose identity isn't known. Many of these strikes violate international law. Maven is not in itself an autonomous weapons system, but it is a large part of the 'kill chain'".

## Bad Business

There are many reasons why it may be in the best interest of tech companies not to contribute to the development of lethal autonomous weapons. First of all, these companies have a social responsibility to ensure that the rapid developments in artificial intelligence are used for the benefit of humankind. The development of lethal autonomous weapons raises many ethical, legal and security concerns, as described in the introduction. Secondly, it is in companies' own interests to ensure they do not contribute to the development of these weapons. Not doing so could lead to severe reputational damage. As Google Cloud CEO Diane Green said, "Google would not choose to pursue Maven today because the backlash has been terrible for the company".[47]

Kevin Roose, technology columnist for The New York Times, argues that there is a substantial financial risk to the tech giants today, as military contracts may be less lucrative than they appear, as they "could come with enormous hidden costs in the form of damaged reputations, recruiting problems and customer boycotts that could swamp any short-term gains. […]But the truth is that tech companies have absolutely no idea how the government will use their products in the future—and how the political landscape might shift, throwing them into an unwanted spotlight. […] Take note, tech giants. Turning down controversial military and government contracts won't doom your business. In fact, in the long run, your shareholders might thank you".[48]

Finally, another reason for tech companies to think twice is the role of tech workers. As mentioned above, there is a growing group that is increasingly concerned about lethal autonomous weapons. Not speaking out on the issue could mean a company loses highly skilled employees. According to Forbes, "In artificial intelligence, particularly, alarming numbers of talented people are stepping away from jobs they fear have negative social consequences".[49] As tech workers are a crucial asset, listening to their views is essential. That is why it is imperative that companies draw a clear line on what their products can and cannot be used for.

"Professional codes of ethics should also disallow the development of machines that can decide to kill a human"

Stuart Russell, professor of computer science at University of California, Berkeley[50]



## Setting Standards

Within the tech sector, various initiatives have developed to ensure that new technology is used for good and to benefit society. For example, the Institute of Electrical and Electronic Engineers (IEEE) developed the Global Initiative on Ethics of Autonomous and Intelligent Systems, which aims "To ensure every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity".[51] It has published the first edition of its 'Ethically Aligned Design', which also includes a section on autonomous weapons. It states that "professional ethics about such systems can and should have ethical standards covering a broad array of issues arising from the automated targeting and firing of weapons". It recommends that "designers not only take stands to ensure meaningful human control, but be proactive about providing quality situational awareness to operators and commanders using those systems".[52]

Many large tech companies have ethics codes or principles related to AI, but most do not mention the military application of their technology, or more specifically autonomous weapons.[53] One exception is Google, whose AI principles mention weapon systems as outlined above. There are also a number of initiatives coming from partnerships between science, industry and NGOs. Examples are Tenets (2016) by the Partnership on AI,[54] and the Montreal Declaration for a Responsible Development of Artificial Intelligence (2018).[55] Neither of these includes a reference to military applications. Another initiative is the Asilomar AI Principles (2017) by the Future of Life Institute, which does include a reference to the military application with the principle "An arms race in lethal autonomous weapons should be avoided".[56]

## What can the Tech Sector Do?

There are a number of steps that tech companies can take to prevent their products contributing to the development and production of lethal autonomous weapons.

- Commit publicly to not contribute to the development of lethal autonomous weapons.[57]
- Establish a clear policy stating that the company will not contribute to the development or production of lethal autonomous weapon systems. This policy should include implementation measures such as:
  - Ensuring each new project is assessed by an ethics committee;
  - Assessing all technology the company develops and its potential uses and implications;
  - Adding a clause in contracts, especially in collaborations with ministries of defence and arms producers, stating that the technology developed may not be used in lethal autonomous weapon systems.
- Ensure employees are well informed about what they work on and allow open discussions on any related concerns.

### What can Tech Workers Do?

Of course, tech workers can also take action themselves. The Campaign to Stop Killer Robots specifically calls on them:

> *"While our campaigners are creating pressure at the United Nations and in national capitals around the world, lobbying governments to enact proactive policy on this issue, we need industry and tech workers to contribute to the conversation and use their technical expertise to drive policy changes. We've seen the power that organizing within companies can have. It's up to each of us to harness the power of community to create meaningful change. [...] The Campaign to Stop Killer Robots stands by to amplify your efforts and ensure they impact international policymakers. There are many forces working against us, but together, we can contribute to a positive future for the industry you work in—one that enshrines human dignity and rights for all".*[58]

"We cannot hand over the decision as to who lives and who dies to machines. They do not have the ethics to do so. I encourage you and your organizations to pledge to ensure that war does not become more terrible in this way."

Toby Walsh, professor of Artificial Intelligence at the University of New South Wales in Sydney



# 3. Technology for Increasingly Autonomous Weapons

## 3.1 Introduction

The history of technology has been characterized by innovations in the military being adapted for civilian applications. For example, many information and communication technologies (ICT) that are commonplace were funded by the US Defense Advanced Research Projects Agency (DARPA), or their equivalents in other countries. Well-known examples are the origins of the Internet (ARPANET) and satellite navigation (GPS).[59] Today, a number of applications in the area of artificial intelligence can also be linked to funding by DARPA.[60]

Many such new technologies that were introduced in the consumer market have then been further developed and adapted to include a much wider range of applications. For example, navigational apps on smartphones have not only replaced paper maps, they can also tell us how to most efficiently get to a destination accounting for real time conditions, suggest alternate means of transport, and include nearby restaurants and entertainment. The precise satellite information required for these digital maps was classified or at least prohibitively expensive just 15 years ago.

Even so, much of the ICT that has changed modern lives significantly over the past few decades emerged purely out of commercial interest. Companies such as Alibaba, Apple, Huawei, Microsoft and Google did not need military-led inventions to become the giant companies they are today. In fact, a new generation of technology is principally driven by private-sector investment, although the nexus between military interests and commercial technology is clear (for example in robotics, artificial intelligence and quantum computing). The military acquisition process is characterised by lengthy development cycles aimed at rather static technologies and platforms rather than the rapid iterative and incremental development cycles required for e.g. modern unmanned systems.[61]

This has led the military to increasingly look to the commercial sector to address its most immediate needs: "Autonomous technologies, originating in the civil sector but adapted for military applications, are likely to become key components of the autonomous drones and weapons of the future. Military planners are aware of the civil sector's lead in developing artificial intelligence and

autonomous systems and are keen to have a slice of the cake".[62]

Whereas the slow military procurement process already discourages many companies from bidding for military contracts, the high financial and political costs associated with breaking into the military domain are also often seen as making the contracts not worth the effort. That was clear especially with the controversy about Google's participation in Project Maven, discussed in the previous chapter, which demonstrated the unease within the sector about contributing to potentially lethal military applications.[63]

Nevertheless, military-funded research and development (R&D) continues to be a key incubator for many new technologies, some purely for military use, others with more diffuse or 'dual-use' applications (military and civilian). Whether it is hardware, such as autonomous vehicles and sensor equipment, or less tangible technologies (human-machine teaming,[64] machine learning etc.), the military prioritises the development of such technologies for specific warfighting applications. Typically, such work is shared by both 'traditional' arms producers and relative newcomers to the military sector, start-ups as well as big tech companies.

Especially, "two separate uses for AI and autonomous technology are becoming increasingly important in the military world. Firstly, autonomous systems can be used to process and analyse large amounts of raw intelligence information in order to find targets. Secondly, AI can be incorporated into the weapons themselves as well as to execute operational missions".[65]

The following sections will look at a number of technologies that are relevant in the development of lethal autonomous weapons, and at the companies that are working on these technologies. As mentioned in the introduction, this does not mean these companies are contributing to the development of such weapons. However they need to be aware of that potential in their technology and they need to have policies to ensure that their technology will not eventually end up in lethal autonomous weapons.

We look at how various parts of the tech sector are involved in technologies that have military relevance, and how these could contribute to increasingly autonomous weapons. This includes computer hardware (e.g. supercomputers, cloud infrastructure, AI chips), as well as the AI software that makes the hardware run. Think for example of visual equipment which in real-time can distinguish potential targets in crowded spaces based on facial recognition – or other software that can identify relevant battle information. Think of increasingly autonomous aerial or ground vehicles, alone or operating in 'swarms', which, fed by such information, can select and attack targets on their own. For long such scenarios used to be science fiction, but they are now quickly becoming reality.

Some of the surveyed companies are small start-ups focusing mainly on military work, while some large tech companies conduct research in consumer applications that may have the potential to enhance warfighting applications. Often, companies actually cover more than one such area of work, and the boundaries between these areas of work are not always clear-cut. However, they are examples that serve to show how many key tech companies have developed technologies that have become increasingly of interest to the military. Certainly, this is not necessarily problematic. However, it is important that companies (themselves and their staff) ensure that their technology will not be used for the development of lethal autonomous weapons that could become part of an AI arms race where human control over the use of force fades away.

The survey questions are copied in the annex of this report.



Companies have been ranked by levels of concern. The ranking was based on three criteria:

1. Is the company developing technology that could be relevant in the context of lethal autonomous weapons?
2. Does the company work on relevant military projects?
3. Has the company committed to not contribute to the development of lethal autonomous weapons?

In the following sections we look at a number of aspects and technologies relevant in the context of emerging lethal autonomous weapons. First we look into some of the largest tech companies, which mostly work on a range of technologies including AI. We then look into relevant hardware, AI architecture, pattern recognition technologies as well as autonomous drones and ground robots.[66]

## 3.2 Big Tech

A number of the successful ICT start-ups of the late 20th century have grown to become multinational companies whose operations extend far beyond their original products. From a highly successful search engine, Google has expanded its activities to include everything from email and data storage to watches and self-driving vehicles. Likewise, Amazon, Apple and Microsoft grew from e-store, personal computer maker and operating system builder respectively into the giant companies they are now, offering a host of digital services and hardware. Similar developments, even though they picked up later, are happening in China, where for example Alibaba started as an online market place and has now expanded into many other areas of work, including cloud computing and payment on the basis of facial recognition. In all cases, progress in the area of artificial intelligence has given these developments a new dimension—and the military is clearly looking at the sector to capitalise on them.

Most of the technologies and services these companies offer are intended for the civilian market but could be repurposed for military applications. In this section we briefly look at the US companies in the context of their work on cloud computing, as well as some of the biggest Chinese companies, plus Samsung and Siemens.[67]

### JEDI

As was mentioned in the previous chapter, Amazon Web Services and Microsoft are the two remaining competitors after Oracle and IBM failed to qualify for the USD 10 billion JEDI project.[68] The JEDI cloud will serve as the infrastructure spanning the Pentagon offices to soldiers in the field. "As opposed to a vast set of incompatible databases that they have in the field now, the deal envisions a unified cloud providing access to data through a range of devices to make decisions on the fly, using machine learning".[69] Even though the JEDI cloud will have many applications that may not be controversial, there is a clear danger for it to play a role in the functioning of autonomous weapons systems, for example to rely on for target identification purposes or other potential cloud-based information. As mentioned in the previous chapter the Chief Management Officer of the JEDI project has explained: "This program is truly about increasing the lethality of our department".[70] Therefore the company that gets awarded the bid should make explicit what its technology can and cannot be used for.

**Amazon's** cloud business alone has generated USD 600 million in classified work with the Central Intelligence Agency since 2014, according to Bloomberg.[71] From the start of the process, Amazon

## Table:
COMPANIES SURVEYED FOR THIS REPORT

Companies have been ranked by levels of concern. The ranking was based on three criteria:

1. Is the company developing technology that could be relevant in the context of lethal autonomous weapons?
2. Does the company work on relevant military projects?
3. Has the company committed to not contribute to the development of lethal autonomous weapons?

| COMPANY | BEST PRACTICE | MEDIUM CONCERN | HIGH CONCERN | HQ | RELEVANT TECHNOLOGY | RELEVANT MILITARY/ SECURITY PROJECTS | COMMIT TO NOT DEVELOP |
|---|---|---|---|---|---|---|---|
| **AerialX** | | | ■ | Canada | Counter-drone systems | DroneBullet | |
| **Airobotics** | | ■ | | Israel | Autonomous drones | Border security patrol bots | |
| **Airspace Systems** | | | ■ | US | Counter-drone systems | Airspace interceptor | |
| **Alibaba** | | ■ | | China | AI chips, Facial recognition | - | |
| **Amazon** | | | ■ | US | Cloud, Drones, Facial and speech recognition | JEDI, Rekognition | |
| **Anduril Industries** | | | ■ | US | AI platforms | Project Maven, Lattice | |
| **Animal Dynamics** | ■ | | | UK | Autonomous drones | Skeeter | X |
| **Apple** | | ■ | | US | Computers, Facial and speech recognition | - | |
| **Arbe robotics** | ■ | | | Israel | Autonomous vehicles | - | X |
| **ATOS** | | ■ | | France | AI architecture, cyber security, data management | - | |
| **Baidu** | | ■ | | China | Deep learning, Pattern recognition | - | |
| **Blue Bear Systems** | | | ■ | UK | Unmanned maritime and aerial systems | Project Mosquito/LANCA | |
| **Cambricon** | | ■ | | China | AI chips | - | |
| **Citadel Defense** | | | ■ | US | Counter-drone systems | Titan | |
| **Clarifai** | | | ■ | US | Facial recognition | Project Maven | |
| **Cloudwalk Technology** | | ■ | | China | Facial recognition | - | |
| **Corenova Technologies** | | | ■ | US | Autonomous swarming systems | HiveDefense, OFFSET | |
| **DeepGlint** | | ■ | | China | Facial recognition | - | |
| **Dibotics** | | ■ | | France | Autonomous navigation, Drones | 'Generate' | |
| **EarthCube** | | | ■ | France | Machine learning | 'algorithmic warfare tools of the future' | |
| **Facebook** | | ■ | | US | Social media, Pattern recognition, Virtual Reality | - | |
| **General Robotics** | ■ | | | Israel | Ground robots | Dogo | X |
| **Google** | ■ | | | US | AI architecture, Social media, Facial recognition | - | X |
| **Heron Systems** | | | ■ | US | AI software, ML, Drone applications | 'solutions to support tomorrow's military aircraft' | |
| **HiveMapper** | ■ | | | US | Pattern recognition, Mapping | HiveMapper app | X |
| **IBM** | | ■ | | US | AI chips, Cloud, Super computers, Facial recognition | Nuclear testing super computers, ex-JEDI | |
| **Innoviz** | | ■ | | Israel | Autonomous vehicles | - | |
| **Intel** | | | ■ | US | AI chips, UAS | DARPA HIVE | |
| **Megvii** | | ■ | | China | Facial recognition | - | |
| **Microsoft** | | | ■ | US | Cloud, Facial recognition | HoloLens, JEDI | |
| **Montvieux** | | | ■ | UK | Data analysis, Deep learning | 'Revolutionise human information relationship for defence' | |
| **Naver** | | ■ | | S. Korea | 'Ambient Intelligence', Autonomous robots, Machine vision systems | - | |
| **Neurala** | | ■ | | US | Deep learning neural network software | Target identification software for military drones | |
| **Oracle** | | | ■ | US | Cloud, AI infrastructure, Big data | ex-JEDI | |
| **Orbital Insight** | | ■ | | US | Geospatial analytics | - | |
| **Palantir** | | | ■ | US | Data analytics | DCGS-A | |
| **Percepto** | | ■ | | Israel | Autonomous drones | - | |
| **Roboteam** | | | ■ | Israel | Unmanned systems; AI software | Semi-autonomous military UGVs | |
| **Samsung** | | ■ | | S. Korea | Computers and AI platforms | - | |
| **SenseTime** | | | ■ | China | Computer vision, Deep learning | SenseFace, SenseTotem for police use | |
| **Shield AI** | | | ■ | US | Autonomous (swarming) drones | Nova | |
| **Siemens** | | ■ | | Germany | AI, Automation | KRNS, TRADES | |
| **Softbank** | ■ | | | Japan | Telecom, Robotics | - | X |
| **SparkCognition** | | | ■ | US | AI systems, Swarm technology | 'works across the defense and national security space in the U.S.' | |
| **Synesis** | | | ■ | Belarus | AI- and Cloud-based applications, Pattern recognition | Kipod | |
| **Taiwan Semiconductor** | | ■ | | Taiwan | AI chips | - | |
| **Tencent** | | ■ | | China | AI applications, Cloud, ML, Pattern recognition | - | |
| **Tharsus** | | ■ | | UK | Robotics | - | |
| **VisionLabs** | ■ | | | Russia | Visual recognition | - | X |
| **Yitu** | | | ■ | China | Facial recognition | Police use | |

■ **HIGH CONCERN** Company working on military/security applications of relevant technologies + chose not to answer our survey's questions in a meaningful way.

■ **MEDIUM CONCERN** Company working on military/security applications of relevant technologies + answered that it was not working on lethal autonomous weapons; or Company not known as working on military/security applications of relevant technologies + chose not to answer our survey's questions in a meaningful way.

■ **BEST PRACTICE** Company answered to explain its policy on how it ensures its technology is not contributing to lethal autonomous weapons.

\- Unknown.

**NB:** This table ranks companies according to the level of concern regarding their potential (unintended) contribution to the development of lethal autonomous weapons. It does not take into account other concerns regarding privacy, human rights and other issues.

has been perceived as the likely winner of the JEDI contract; it has even been suggested that that the invitation tender was written so that only Amazon could win.

Jeff Bezos, Amazon's chief executive, said in the context of Google's withdrawal from Project Maven: "If big tech companies are going to turn their back on the U.S. Department of Defense, this country is going to be in trouble".[72] However, there is a big difference between turning your back on your country's national defence and making sure that your technology will not enhance or become part of lethal autonomous weapons.

**Microsoft** CEO Satya Nadella has also strongly defended their policy on military contracts: "We will have our own committee that will really direct us in terms of what engagements we do or don't do, and especially when it comes to the United States and liberal democracies at large, we will rely on our democratic process and the institutions that we work with and their own ethics as well". He also said that the US "armed forces have a fundamental grounding on what it means to deploy any technology or practice which is ethically used".[73] What that fundamental grounding is remains unclear. The fact is that Google concluded that it "couldn't be assured that [JEDI] would align with our AI Principles".[74] As mentioned in the previous chapter: Microsoft employees appear ready to protest in case their company would win the JEDI contract.

In 2018 Microsoft published "The Future Computed," examining the applications and potential dangers of AI. It argues that strong ethical principles are necessary for the development of AI that will benefit people, and defines six core principles: "fair, reliable and safe, private and secure, inclusive, transparent, and accountable".

But, as Microsoft employees argue: " With JEDI, Microsoft executives are on track to betray these principles in exchange for short-term profits. If Microsoft is to be accountable for the products and services it makes, we need clear ethical guidelines and meaningful accountability governing how we determine which uses of our technology are acceptable, and which are off the table. Microsoft has already acknowledged the dangers of the tech it builds, even calling on the federal government to regulate AI technologies. But there is no law preventing the company from exercising its own internal scrutiny and standing by its own ethical compass. "[75]

**Oracle Corporation** sells database software and technology, cloud-engineered systems, and enterprise software products, including database management systems. In 2018, Oracle was the world's third-largest software company by revenue.[76] Moreover, "Oracle makes it easy for enterprises to realise value from artificial intelligence and machine learning (ML)".[77] In the military sphere, "Oracle helps modern defense prepare for dynamic mission objectives".[78] This includes, for example, cloud contracts. Oracle bid for the Pentagon's JEDI contract and filed multiple complaints in the course of the process, in part contesting the decision to have a single cloud vendor for years, which it sees as uncompetitive.[79]

**IBM,** the fourth original main contender for the JEDI contract, is discussed in the next section.

Amazon and Oracle did not respond to multiple requests to take part in our survey so their stance on lethal autonomous weapons remains unclear. Whereas Microsoft research director Eric Horvitz (see previous chapter) did respond, his views cannot be taken as the company's position. Their lack of response combined with their military links means these three companies qualify for the label 'high concern' in the context of this report.



## BAT

Meanwhile, China's largest tech companies Baidu, Alibaba and Tencent—also collectively known as BAT—are making extraordinary gains in artificial intelligence with "the support, investment and commitment of the Chinese government to become the dominant AI player in the world".[80]

**Baidu** is the largest provider of Chinese-language Internet search services and is highly committed to artificial intelligence and machine learning. It is exploring applications for artificial intelligence and machine learning, "including in their offices where facial recognition technology makes standard ID cards unnecessary and allows you to order tea from a vending machine".[81]

In 2013, Baidu opened an AI research lab in Silicon Valley and, like Google, has been investing heavily in many applications of AI, from automated personal assistants to autonomous cars and health care.[82] However, with the ongoing trade row between the US and China, Chinese investors and companies, including the BAT trio, appear to be scaling down their activities in Silicon Valley.[83]

At the same time, the Chinese government is stepping up its strategy of leveraging ways to cooperate on dual-use technologies, including in AI and automation, enlisting technology companies and universities, including Baidu, to promote their military application.[84]

Baidu is leading China's National Engineering Laboratory for Deep Learning Technologies, established in March 2017, which will pursue next-generation research in deep learning. Baidu will also contribute to the National Engineering Laboratory for Brain-Inspired Intelligence Technology and Applications, which aims to develop AI technologies that learn from the mechanisms of the human brain and to promote brain-inspired neural chips and brain-inspired intelligent robotics.[85]

**Alibaba,** China's largest online shopping company, has recently invested in "seven research labs that will focus on artificial intelligence, machine learning, network security, natural language processing and more".[86] In September 2018, Alibaba announced that it had established a semiconductor subsidiary, called Pingtouge, to focus on customised AI chips and embedded processors. Alibaba is also a major investor in the tech sector, for example in companies such as Megvii and SenseTime, mentioned elsewhere in this report.[87] Interestingly, while having no apparent direct link to the military itself, Jack Ma, the co-founder and executive chairman of Alibaba, is well aware of the tensions and risks of the digital revolution. With machine learning and artificial intelligence eliminating jobs, "the third technology revolution may cause the Third World War", he said in 2017.[88]

**Tencent**, founded in 1998, is China's biggest social media company,[89] but has also set up the Miying platform to assist doctors with the screening of diseases, among other things.[90] One of the company's slogans is 'AI in all'.[91] Its focus is on research in machine learning, speech recognition, natural language processing and computer vision and on developing practical AI applications in online games, social media and cloud services. It is also investing in AI technologies to be used in autonomous vehicles.

Tencent favours an approach to ethics that not only allows socially beneficial uses of AI for medical purposes or agriculture but also ensures a "social contract" between companies and users to govern the use of personal data. "Billions of users have entrusted us with their personal sensitive information; this is the reason we must uphold our integrity above the requirements of the law".[92]

Neither Baidu, Alibaba nor Tencent responded to our survey, so their stance on lethal autonomous weapons remains unclear.

### ELECTRONICS AND AI

Companies more commonly known as consumer electronics or industrial tech producers - and to a lesser extent as military producers - are also investing heavily in AI and robotics. Much like previously mentioned ICT companies, the technology they develop could potentially be used as a key component for lethal autonomous weapons. Samsung and Siemens are two major examples of such industrial tech producers.

**Samsung** is one of the world's largest tech companies and South Korea's largest chaebol (business conglomerate). As part of its quest to stay a leading producer of telephones and computers, it is also developing AI technologies to be applied to all its products and services. Its primary goal is "to secure cutting-edge AI core technologies and platforms—human-level AI with the ability to speak, recognise, and think—to provide new AI-driven experiences and value to its customers. Aligned with our goal above, we are conducting research in broad thematic areas such as AI core algorithms, on-device AI, next-generation virtual assistant platform, and so on".[93]

Samsung Techwin used to be the military arm of Samsung and was known for its SG1A Sentry robot, but that division was sold to Hanwha in 2014.

Samsung did not respond to requests to participate in our survey so their stance on lethal autonomous weapons remains unclear.[94]

**Siemens**, headquartered in Germany, is Europe's largest industrial manufacturing conglomerate and is known for its medical diagnostics equipment (CT Scanners), energy equipment (turbines, generators) and trains.

In the area of AI, Siemens produces MindSphere, a cloud-based system that can link products, plants, systems and machines, enabling the use of AI in industry. "MindSphere performs extensive analyses to make the vast amounts of data generated by the Internet of Things (IoT) useful for optimisation, simulation, and decision-making", according to the company.[95]

In 2013 Siemens won a contract with Carnegie Mellon University and HRL Laboratories "on a military research project to unlock secrets in the nature of knowledge in an effort to improve tools and training available to intelligence analysts".[96] The USD 2.2 million contract was part of the Knowledge Representation in Neural Systems (KRNS) programme of the Intelligence Advanced Research Projects Agency (IARPA)—the intel counterpart of DARPA—to develop "systems that aim to predict patterns of neural activity associated with particular concepts and that can interpret which concepts are represented within measured patterns of neural activity".[97]

Siemens Corporate Technology is also working with DARPA on the TRAansformative DESign (TRADES) programme. "The goal of the multimillion dollar project is to develop a new digital modelling technology that will expand existing computer-aided design (CAD) software to design incredibly complex objects with superior functional properties that can still be manufactured with current manufacturing processes".[98]

In response to our autonomous weapons survey Siemens mentions that it feels it is important to have "such an ethical debate and it should be guided by people with expertise in that field".

The company added that "Siemens is not active in this business area. Where we see a potential risk that components or technology or financing may be allocated for a military purpose, Siemens performs a heightened due diligence. [...] All our activities are guided by our Business Conduct Guidelines that make sure that we follow high ethical standards and implement them in our everyday business. We also work on responsible AI principles which we aim to publish later this year".[99] Siemens has been ranked as medium concern, as they state that they are not active in this business area, but they do not have a policy that explicitly says that they will not contribute to the development of lethal autonomous weapons.

## 3.3 Hardware

Computer hardware producers may also be linked to the potential development of lethal autonomous weapons, especially as advanced computing requires advanced 'workhorses'. For example, supercomputing technology is key to further breakthroughs in artificial intelligence, as much as it has been "a mainstay of military and intelligence agencies, used for chores ranging from cracking codes to designing nuclear weapons", as well as civilian uses such as weather prediction and other simulation applications.[100] While the US is still producing the world's most powerful supercomputers, China has taken over in terms of numbers: 227 or 45 per cent of the world's 500 most powerful supercomputers are in China, as opposed to 109 or 22 per cent in the US.[101]

Just as supercomputers have played a leading role for decades in the development of computing models used for complicated forecasting or other heavy-duty computing, artificial intelligence and the digestion and analysis of large amounts of information ('big data'[102]) will take computing requirements to a new level. Companies producing chips or semiconductors have also been crucial in AI progress. The incorporation of graphics processing units (GPUs) in the early 2010s aided the deep-learning revolution.[103]

Military uses of hardware include the validation of simulation models, enabling manufacturers "to widen the scope of their tests because it can be difficult to test autonomy in a physical incarnation for reasons including safety constraints—particularly if the system is weaponised—and the potential security implications of putting new capabilities through their paces in the real world".[104]

Such developments can also be important for developing and testing lethal autonomous weapons.

One of the oldest computer producers is **IBM**, which is now following "a very aggressive roadmap" towards producing "next-generation artificial intelligence chips" and building a new AI research centre for that purpose, according to one of its AI research directors.[105] The company's researchers expect to improve AI computing performance by 1,000 times over the next 10 years and to "support the tremendous processing power and unprecedented speed that AI requires to realise its full potential".[106]

IBM has a long history of military contracting. "When public security is jeopardised by disaster or military threat, defence and intelligence forces need to move from data to decision in minutes. IBM analytics, machine learning and artificial intelligence solutions can give your forces the tactical edge to generate and share actionable intelligence in a timely manner for a safer world".[107] Working towards that safer world also appears to include building supercomputers for nuclear weapons research and simulations, including the Sequoia and Sierra.[108] Furthermore, IBM is doing augmented intelligence work for the US Marine Corps.[109]

IBM's Watson design lead Kathryn McElroy and Guruduth Banavar, Vice-President of Cognitive Computing at IBM Research, were among three dozen IBM staff who signed an open letter in 2015 calling for a ban on autonomous weapons.[110] In response to the survey IBM confirmed that they are currently not developing lethal autonomous weapons systems. For this reason they are ranked as medium concern, as to be 'best practice' IBM would also need to ensure that its technology will not be used in these weapons.

Probably best known for its computer processors, **Intel** works on various AI technologies, including specific solutions, software and hardware.[111] Intel provides these services to governments. "As budgets grow tighter, Intel AI can empower government agencies and their partners to do more with less. Combined with deep learning, satellite images and overhead video can unlock new possibilities in defence, disaster response, and mapping".[112]

In 2017, Intel was selected by DARPA "to collaborate on the development of a powerful new data-handling and computing platform that will leverage machine learning and other artificial intelligence techniques".[113] The project is called DARPA HIVE, a joint research programme between Intel and DARPA valued at more than USD 100 million over the 4.5 years that it will run. In July 2018, it was announced that Intel will be working with DARPA on developing "the design tools and integration standards required to develop modular electronic systems".[114]

Additionally, Intel has invested significantly in unmanned aerial vehicles (UAV) and flight control technology, focusing on industrial inspection, surveying and mapping for civilian purposes, which could provide defence applications too. For example, it has developed the Shooting Star system, a lightshow capability that enables a single pilot to launch a swarm of UAVs that can position themselves without a GPS signal—a capability desired by military users too.[115] In 2016 it acquired the German UAV company Ascending Technologies (AscTec).

Intel did not respond to repeated requests to take part in our survey on their position regarding autonomous weapons.

## 3.4 Aİ Software and System İntegration

Many companies specialise in conducting research and development into artificial intelligence, often encompassing various sub-fields of AI such as machine learning. Amazon, for instance, places high priority on machine learning; without it they would not be able to grow their business and optimise their "logistic speed and quality", among other things.[116]

Clearly, the military has a big interest in these areas too. Currently NATO initiatives are underway to integrate augmented reality (AR) and artificial intelligence solutions into existing ground personnel mission suites to enhance their operational effectiveness and to assist in situational awareness, target acquisition and route finding. Practical progress remains slow despite significant technology injections from the commercial sector, according to military magazine Jane's Defence Weekly.[117]

A leading force is the US Special Operations Command, which uses developments in AR, AI and ML to support "synthetic training and operational environments".[118] Specific areas of interest include mission rehearsal support and targeting, holographic displays, gaming technologies and neuromorphic computing. "We know that AI and autonomy will sharply bend the forward operating environment arc toward unimagined efficiencies and surprising challenges", said a US military official.[119]

The US Air Force has similar interests and is actively connecting with start-ups. Earlier this year, at a meet-up where companies could pitch innovative ideas and technologies, more than 50 companies immediately received USD 3.5 million in initial funding, with another USD 5 million to be paid out in instalments. With cash and a minimum of red tape, the Air Force is looking to eliminate concerns that the Pentagon is very much aware of. As Will Roper, assistant secretary of the Air Force for acquisition, technology and logistics, said: "We've got to learn a different language, one that doesn't involve much talk of war and weaponry".[120]
One such company the Pentagon is connecting with is **CrowdAI**, which has "mixed machine learning with mapping technology to identify flooded Texas roadways in the aftermath of Hurricane Harvey, or decimated buildings after bombings in Aleppo".[121] It has already received a small grant from the US Air Force, which the company hopes to expand into a proper military contract. However, asked by tech magazine Wired if there are some applications of the tool that CEO Devaki Raj would consider off limits, she said yes, but declined to name any in particular, saying instead, "We would like to make sure our technology is used for good".[122]

One company that has turned down government offers is **Affectiva**, an "artificial emotional intelligence" start-up whose software uses AI to track human emotions. One such offer was from a venture fund backed by the CIA, which wanted to use the product to improve their surveillance capabilities. Affectiva has since been successful with nongovernmental projects and has made ethical AI use a core part of its brand. "We wanted to be trusted," said co-founder Rana el Kaliouby, "We used the core value of integrity and respecting people's privacy as a way to weed out use cases".[123]

Silicon Valley's **Palantir** supplies 'Palantir Intelligence', "a complete, proven solution that is used throughout the intelligence community to efficiently, effectively, and securely exploit and analyse data, leading to more informed operational planning and strategic decision-making".[124]
It is also "a developer of increasing common predictive policing technology that's used by law enforcement agencies around the United States".[125] The data-analysis company was founded in 2004 by Trump adviser Peter Thiel and has roots in the CIA-backed In-Q-Tel venture capital organisation.[126]
In March 2019, it was revealed that the US Army had awarded Palantir a contract "to build out and deploy an artificial intelligence system that can help soldiers analyse a combat zone in real time", also known as the Distributed Common Ground System (or DCGS-A, for Army).[127]
The software company had beaten a rival bid from Raytheon, one of the world's largest arms producers. The estimated more than USD 800 million contract is the company's largest-ever defence deal.[128]

In 2016 it had already won a USD 222 million deal from the Special Operations Command (SOCOM) for a technology and logistics software and support project called "All-Source Information Fusion", meant to bring together information gathered by SOCOM.[129]

**Anduril Industries**, founded in 2017, is one of the more vocal businesses advocating stronger ties between the tech sector and the Pentagon: "AI has paradigm-shifting potential to be a force-multiplier […] it will provide better outcomes faster, a recipe for success in combat".[130]
Thus, while Google withdrew, Anduril has eagerly continued working on Project Maven, plus offered support for the Pentagon's newly formed Joint Artificial Intelligence Center.[131]

One of the company's co-founders is Trae Stephens, a former intelligence official. According to Stephens, the reluctance of many tech companies to bid for military contracts is merely a matter of semantics. He thinks the Pentagon has made its life unnecessarily difficult by using terms like attack or lethality in project descriptions. "We just can't use this word. You're not going to win being like: 'Our priority is soldier lethality'", Stephens said. "[…] There's this slight conflict of semantic culture. It's just kind of silly, and we should like stop making unforced errors".[132]
Clearly, Stephens ignores the fact that originally neither Project Maven nor JEDI were overtly militaristic, but resistance against the projects emerged after people at Google and Microsoft started to understand what was included in the (potential) purposes of the work.
Anduril's website mentions that it "is pioneering life-saving AI platforms for protecting troops, performing search & rescue missions, fighting drug cartels, defending energy resources, combating wild fires, stopping human traffickers and much more".[133]

Its key concept is the Lattice, which comes as a tower or as an unmanned aerial system. The "ground-breaking software + hardware system […] uses cutting-edge AI, machine vision and mesh networking to solve critical problems and save lives. Lattice integrates all Anduril hardware and third party sensors into a single, autonomous operational platform. […] Lattice's revolutionary AI-powered sensor fusion allows all device sensors to act as one large sensor".[134]

The technology is designed to provide a view of the front lines to soldiers, "including the ability to identify potential targets and direct unmanned military vehicles into combat", according to The Intercept.[135] In tests, Lattice has reportedly helped border agents catch numerous people crossing the border.[136]

Another Anduril co-founder is Palmer Luckey, previously one of the founders of Oculus VR, which was bought by Facebook in 2014 for USD 2 billion. Anduril is now "'deployed at several military bases. We're deployed in multiple spots along the U.S. border,' according to Luckey, cryptically adding: 'We're deployed around some other infrastructure I can't talk about'".[137]

Despite a specific question on autonomy and human control in their Lattice technology, a media company handling Anduril's external affairs answered in response to our survey request: "Given that this isn't the company's focus, we won't be able to help with the survey".[138]

**SparkCognition**, from Austin, Texas, is an artificial intelligence company that partners "with the world's largest organisations that power, finance, and defend our society to uncover their highest potential through the application of AI technologies".[139] The company has attracted the interest of former and current Pentagon officials. Most recently, Robert Work, former Deputy Secretary of Defense joined the company's advisory board.[140] Retired Marine Corps General John Allen is a board member. Among the firm's senior corporate advisers is Wendy Anderson, who served as chief of staff for then Deputy Defense Secretary Ash Carter and as deputy chief of staff for then Defense Secretary Chuck Hagel.[141]

SparkCognition works "across the national security space—including defense, homeland security, intelligence, and energy—to streamline every step of their operations".[142] Outside the US, they have worked with the British Army to advance artificial intelligence applications, specifically "on the role of machine learning in military applications and [to] contribute to research on future military planning. This partnership focuses on how operations can be streamlined using AI technologies today".[143] Founder and CEO Amir Husain and his colleague August Cole are active participants in the debate about AI, warfare and how the Pentagon and industry should adapt. In one of their articles they describe a "defensive mothership-swarm operational concept of swarming drones" to counter a hypothetical Russian attack, and conclude that "there are technical challenges, to be sure, such as power management or deploying a cheap-and-resilient global sensing network. But they are not insurmountable, nor is this kind of countermeasure hypothetical. In fact, SparkCognition began working on this very swarm-mothership concept a few years ago and has filed U.S. patents covering the design of such systems. Moreover, the same advances in machine-learning algorithms that make drone-launching robot submarines a reality can also create global data-gathering networks based on sensors that cost less than last year's mobile phone".[144]
Clearly also, what is described here as 'defensive' could be applied to offensive concepts too, as they implicitly acknowledge: "AI and robotics […] already allow U.S. asymmetric responses that are inexpensive, resilient and globally scalable. Ultimately, though, the biggest challenges with autonomy and robotics will not be technological. It will be our willingness to break with convention".[145] The notion of a global arms race and how this could spiral out of control appears absent in their thinking.

In another article, Husain and Cole assess that "the most essential Pentagon suppliers will be the ones that master robotics and artificial intelligence. […] Taken together, today's leading digital companies have many of the traits for a reimagined, expanded defense industrial base, one that reflects the social, political, and strategic power of companies such as Amazon, Google, and Facebook. Moreover, the most strategically important machine learning and robotics technologies will likely originate in non-defense firms based on their overall investment, market-driven innovation cycles, and talent acquisition. U.S. defense policy is shifting but the speed of technological advancement remains far faster".[146]

CEO Amir Husain believes that restrictions on autonomous weapons would stifle progress and innovation, and says that a blanket ban is "unworkable and unenforceable". Scientific progress is inevitable, "and for me that is not frightening", he added. "I believe the solution—as much as one exists at this stage—is to redouble our investment in the development of safe, explainable and transparent AI technologies".[147]

Likewise, Wendy Anderson, now responsible for Defense and National Security at SparkCognition, has said that to suggest a ban or even tight restrictions on the development of any technology is a "slippery slope" and would put the United States at a competitive disadvantage, as other countries will continue to pursue the technology.[148] "We cannot afford to fall behind", said Anderson. "Banning or restricting its development is not the answer. Having honest, in-depth discussions about how we create, develop, and deploy the technology is."

With such vocal opinions on how they foresee the tech sector becoming deeply involved developing tools of modern warfare, it is especially unfortunate that SparkCognition did not answer repeated requests to take part in our survey.

Founded in 2015 by former Yahoo executive Ariel Seidman, **Hivemapper** "provides mapping, visualisation, and analytic software tools".[149] It uses video footage to generate instant, detailed, three-dimensional maps and automatically detect changes the human eye cannot. Its maps have been built inter alia for asset tracking and autonomous navigation. Seidman "believes Silicon Valley and the US government have to work together to maintain America's technological edge—lest authoritarian regimes that don't share the US values catch up".[150] The company can "detect and alert the user to changes on the ground

over time; it can pinpoint, say, an enemy truck that wasn't there before".[151]

While Hivemapper has several high-profile military customers, CEO Seidman signed the 2015 Future of Life Institute's open letter.[152] Answering our survey, he also says that he is very aware of the discussion and that it is an important topic. "We build software that helps people build maps so it's not directly relevant. However, we absolutely want to see a world where humans are in control and responsible for all lethal decisions".[153]

Indeed, a tool like Hivemapper could potentially be used to model Air Force bombing, notes a Wired journalist—and that is an ongoing conversation with their staff, says another of the company's directors: "We think it's important that companies going after this are aware of what the use cases are," he says. "We don't want to be throwing our product over the rail and saying, 'Go figure it out.'" Rather ambiguously though, he also says: "just walking away from anything offensive has a lot of longer-reaching impacts [...] Within the confines of the regulations, the law ... our job is to help support [the Air Force] and honor what their mission is".[154]

This leaves the question of what Hivemapper would do if the (US) military decided that some lethal decisions could be left to autonomous weapons, which would potentially implicate Hivemapper's products.

In July 2018 it was reported that the UK company **Montvieux** is developing "a new military decision-making tool known as predictive cognitive system. [...] The military system can be used to assess a wide range of highly complex data that are beyond the ability of analysts to simultaneously comprehend. Using Deep Learning based neural networks, the predictive cognitive control system will be able to make confidence-based predictions of future events and outcomes of direct operational relevance to the defence users".[155] Subsequently, in January 2019, the UK government revealed that "Montvieux receives [...] funding to enhance the protection of forces and improving the efficiency and effectiveness of information collection. [...] The proliferation of data within the military poses a significant challenge for operators interpreting differing data sets into meaningful information upon which to make informed and timely decisions. Artificial Intelligence capabilities are developing at pace and can present opportunities through Deep Learning for operators and decision makers to interpret vast, disparate data sets concurrently".[156]

The French company **EarthCube** "is developing monitoring solutions based on an automated analysis of geospatial information. By combining state-of-the-art AI technics in both Computer Vision and Machine Learning, EarthCube enables its customers to access more precise information, thus ensuring faster and less costly interventions".[157]

EarthCube is also offering applications for military purposes[158] and has been described as "conceiving the algorithmic warfare tools of the future".[159] As the company's CEO says: "With the emergence of new sensors—whether they are satellite, UAV or plane—we have seen here a great opportunity to close the gap between AI in the lab and Activity Based Intelligence (ABI) in the field".[160]

"EarthCube [...] uses the latest advances in medical imagery and artificial intelligence and applies them to automatically classify objects, detect changes and analyze scenes. The objective is to offload the drudge work for image analysts by only offering images which feature whatever it is the analyst is looking for: tanks, combat aircraft, a new building, for example".[161]



Boston-based **Neurala** sells patented AI technology that can run on light devices, "based on advanced research work cofounders Versace, Gorshechnikov and Ames conducted for NASA, DARPA, and the Air Force Research Labs".[162] Neurala "helps bring artificial intelligence to drones, robots, cars, and consumer electronics by helping these devices inspect their environment, make decision and navigate obstacles. The company already works with a broad range of clients including the US Air Force, Motorola and Parrot".[163] Military AI applications for drones are a key focus for Neurala. "When equipped to a military drone, the software could identify a specific target in the field. The system then alerts a human operator that the target may have been located".[164] Clearly, this indicates human involvement, but how does Neurala ensure this will remain the case?
Co-founder and CEO Massimiliano Versace signed the Future of Life Institute's 2017 open letter to the UN,[165] but did not answer requests to participate in our survey.

## 3.5 Pattern Recognition

In computer science, pattern recognition can be divided into various subsections:

- Biometrics: identification of people using e.g. facial, fingerprint and/or iris recognition;
- Linguistics: including language identification, language understanding (e.g. in translating), speech recognition (conversion of the spoken word into text) and voice recognition (identifying the person speaking);
- Textual: e.g. handwriting and character recognition used to convert handwritten or typewritten text into machine-encoded text;
- Gesture recognition: the interpretation of human gestures;
- Activity recognition: the recognition of events;
- Object recognition.[166]

Such technologies can be highly relevant for the development of lethal autonomous weapons, enabling the automatic identification and subsequent attack of targets based on the recognition of certain patterns by AI systems. This section focusses mainly on facial recognition technology.

Ever since surveillance cameras and biometric identification emerged in the public domain, these technologies have caused concerns relating to their impact on the right to privacy and bodily integrity. Recently, San Francisco became the first US city to ban the use by police of facial recognition tech in an apparent effort to halt the "creeping surveillance culture".[167] Similarly, an Aegis facial recognition system launched to track students of a New York school has been called an "unprecedented invasion of privacy" and a waste of money.[168]

The Chinese state, however, is very much embracing these technologies for societal control.[169]
The Muslim-dominant western Xinjiang region in particular is seen as a test laboratory for police and other government agencies as part of the "Strike Hard Campaign against Violent Terrorism".[170]
According to Human Rights Watch, since late 2016 the Chinese government has subjected the 13

million Muslims that live in Xinjiang to mass arbitrary detention and heightened repression in general, with up to one million people being held in "political education" camps.[171]

Globally, big tech companies including Facebook, Palantir and Microsoft are also using such technologies to build systems to document and track potential migrants.[172]

The potential and the impact of facial recognition are huge. Assuming that most technical issues can be solved, its use for personal convenience (for payments and for smartphone access) will likely increase massively. Privacy and human rights issues clearly remain, as the intrusive use in Xinjiang shows, and people in Western democracies in particular do not easily accept mass surveillance technologies. Worse, the use of facial recognition in warfare is looming, based on either individual characteristics or ethnicity, gender, age or some other classification. Taken one step further, such technologies could then be used for autonomous weapons to select and attack specific targets. Companies should therefore ensure that their pattern recognition technologies will not be used for such purposes.

## CHINA'S INDUSTRY

Booming government demand for smart surveillance cameras, voice-recognition technology and big-data analytics has meant big business for China's AI companies; but this has also raised concern that they are contributing to the erosion of civil liberties, as indicated above.[173] Moreover, export is becoming a major focus for Chinese companies.[174]

The Beijing-based artificial intelligence provider **Megvii** was founded in 2011 and is best known for its facial recognition software Face++, which is used by Alibaba's Alipay in facial scanning for making payments. Megvii is said to use facial scans from a Ministry of Public Security photo identification database containing files on nearly every Chinese citizen.[175] Such a private-public partnership shows how what looks a win-win situation for both company and state may not be so clearly beneficial for the private individual. "We want to build the eyes and brain of the city, to help police analyse vehicles and people to an extent beyond what is humanly possible", Megvii has said in the past.[176]

One of Megvii's biggest competitors is **SenseTime**, founded in Hong Kong in 2014, which sells artificial intelligence software that recognises things and people. Its image-identifying algorithms have made it "the world's most valuable AI start-up", worth more than USD 4.5 billion.[177] Various Chinese police departments use its SenseTotem and SenseFace systems to analyse footage and arrest suspects. Government contracts account for about two-fifths of its revenue, according to the company's CEO.[178] SenseTime emphasises that AI is "an extension of human intelligence" with the ultimate goal of benefitting human beings.[179]

Remarkably, SenseTime recently sold its 51 per cent stake in security joint venture Tangli Technology in Xinjiang, a 'smart policing' company it set up with Leon, a major supplier of data analysis and surveillance technology, in November 2017.[180] SenseTime's decision marks the first time a major Chinese tech company has opted out of working in the region.

A third example of China's fast-growing facial recognition industry is **Yitu**, which "integrates advanced AI technology business applications to build a safer, faster and healthier world".[181] One of its products is the 'Intelligent Service Platform', where a "visual intelligence algorithm covers facial recognition, vehicle identification, text recognition, target tracking and feature-based image retrieval". Its Dragonfly Eye System is said to identify a person from a nearly two-billion-picture database in a few seconds.[182] By last year its technology was in use in more than 20 provincial public security bureaus in over 300 cities.

In February 2018, Yitu supplied Malaysia's police with facial recognition technologies, said to be its first deal outside of China.[183] It has also entered into a strategic partnership in the fields of public security, finance and health care with local governments and various organisations in Britain.[184]

Other fast-expanding Chinese companies in this area are **Cloudwalk Technology** and **DeepGlint Technology.** None of the Chinese companies responded to our requests to participate in the survey.

## UNITED STATES CATCHING UP?

These technologies are those where the bias issue is most obvious. For instance, the American Civil Liberties Union ran a test of **Amazon's** Rekognition programme where "nearly 40 percent of the false matches by Amazon's tool, which is being used by police, involved people of colour".[185] The company has also faced much criticism since its partnership with police and government agencies was revealed. The backlash grew after links between Amazon and Immigration and Customs Enforcement (ICE) were reported, raising further concerns that AI face-scanning ID software would be used to aid ICE's deportation programme.[186]

However, Amazon has since "proposed guidelines" for the responsible use of the tech that it hopes policymakers in the US and worldwide will consider when drafting new laws. These include the need of tech to be governed by current laws, including those that protect civil rights, and the need for human oversight when facial recognition is used by law enforcement. The guidelines also stress that the tech should not be the "sole determinant" in an investigation.[187]

Another US company working on facial recognition is **IBM**, whose Diversity in Faces dataset[188] contains information scraped from a million images posted on Flickr under the Creative Commons licence. It was released by IBM and shared with companies and universities linked to militaries and law enforcement across the world. According to NBC News, the people "photographed on Flickr didn't consent to having their photos used to develop facial recognition systems".[189] IBM maintains the project aims to help make facial recognition systems less biased.[190]

IBM has long worked with the US military on video-related technologies, aiming to move from object identification to classifying an event. "The challenge here is to understand why the green truck is there […] Where did it come from? Are there humans around the truck, and why were they there? Did they go into the truck, and if so, where are they going now? That type of reasoning takes much more 'horse power', and they're turning to us for that", according to Joe Cubba, Vice-President for defence and intelligence at IBM's Global Business Services/Public Sector arm.[191] He refers to it as a blend of AI and human analysis, or augmented intelligence, with the technology supporting—not replacing—the human brain, which can then concentrate more on analysis rather than detection.

In July 2018 **Microsoft** was the first tech giant to join a growing call for regulations to limit the use of facial recognition technology. In a blog about the potential uses and abuses of facial recognition, President Brad Smith, compared the technology to products like medicines and cars that are highly regulated. "We live in a nation of laws, and the government needs to play an important role in regulating facial recognition technology", Smith wrote. He added: "A world with vigorous regulation of products that are useful but potentially troubling is better than a world devoid of legal standards".[192]

### RUSSIA AND BELARUS

**Synesis** is a leading Belarussian company with offices in Russia, Kazakhstan and the US, working on the "development and deployment of AI- and Cloud-based applications with millions of users", founded in 2009. It counts IBM and Yandex among its customers.[193] It has developed "a video analytics platform called Kipod that functions like Google Search for video content. Used by law enforcement agencies, governments, and private security organisations, it is able to find human faces, license plates, object features, and behavioural events in massive amounts of footage. What's really unique about their cloud-based service is its scalability: the company claims it can work with one million users, one million cameras, and search one petabyte (a million gigabytes) worth of videos".[194] Kipod is used by law enforcement agencies in Belarus, Russia, Kazakhstan and Azerbaijan[195].
Russia's **VisionLabs** was founded in 2012 and is specialised in "cloud visual solutions" for video surveillance and other applications—its main product is a software package called Luna, which allows businesses to "verify and identify customers instantly" based on photo or video images, thanks to Luna's "unique quality and performance pattern recognition technology".[196] VisionLabs partners with more than ten banking organisations in Russia and the Commonwealth of Independent States (CIS), which use visual recognition products to streamline customer services and prevent credit fraud. It has also partnered with Facebook and Google, building an "open-source computer vision platform".[197]

In response to our survey VisionLabs very clearly explained that they "explicitly prohibit the use of VisionLabs technology for military applications. This is a part of our contracts. We also monitor the results/final solution developed by our partners".[198]

## 3.6 Autonomous Aerial Systems and Swarming Technology

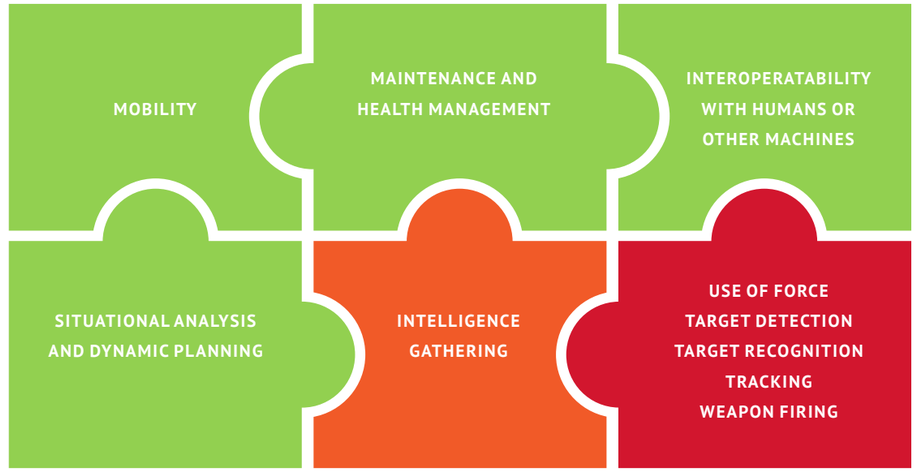
While for a long time technological progress in the area of unmanned aerial systems and vehicles (UAS and UAV, more commonly known as drones) mainly came through military-industrial research, in more recent years a surging civilian demand has spurred developments too.[199] The latter includes both hobby drones and the professional market, e.g. for agricultural or industrial purposes. A wide range of companies are working on unmanned aerial systems, from predominantly commercial ones, including well-known companies such as the Chinese companies Yuneec and DJI, to mainly military companies such as General Atomics and AeroVironment (both in the US) and China Aerospace Science and Technology Corp (CASC). But there is not always a clear dividing line between civilian and military producers, with civilian product types being used for military and security purposes as they become technologically more advanced and cheaper.[200]

On the military side, drone demand has increased over the whole spectrum of sizes (from micro to ultra-large), with ever-improving functionalities, including visual and other sensor capabilities, as well as the potential to weaponize them. For this report, the specific worry is the trend towards more autonomy, not so much in take-off and landing or navigation, but rather regarding features that enable autonomous targeting and attacking. Increasing autonomy in such features is pushing the human operator further away in terms of control over the system, with the risk of them being removed from the decision-making loop altogether.

Or, as a recent report puts it:

> *"Powered by advances in artificial intelligence (AI), machine learning, and computing, we are likely to see the development not only of drones that are able to fly themselves – staying aloft for extended periods – but those which may also be able to select, identify, and destroy targets without human intervention. In many ways, the increasing use of remote controlled, armed drones can be seen as a kind of 'halfway house' towards the development of truly autonomous weapon systems. The incremental way in which drone technology is developing, and the ability to 'bolt on' new features, means that drones are ideally suited to morph into autonomous weapon systems".*[201]

**Figure:**
FUNCTIONS OF AN AUTONOMOUS DRONE




source: https://www.sgr.org.uk/index.php/resources/lethal-and-autonomous-coming-soon-sky-near-you

### AUTONOMOUS DRONES

Indeed, quite a few companies surveyed for this report make what they call autonomous UAVs. Although the meaning of 'autonomous' may vary considerably, some do appear to be increasingly close to lethal autonomous weapon systems.

**Animal Dynamics**, a spin-off company originating in the University of Oxford Zoology Department, develops UAVs inspired by "evolutionary biomechanics".[202] Its powered, unmanned paraglider called Stork has "autonomous guidance and navigation in both GPS and GPS-denied environments".[203] According to its CEO, Alex Caccia, its "autonomy is focused on following the mission plan, obstacle avoidance, and collision avoidance, and the mission intent is at all times human".[204] While still under trial, the unmanned aerial delivery vehicle has received interest from humanitarian aid/disaster relief organisations and various military organisations. In 2018, the Stork was tested in live logistical experiments as part of the 'Autonomous Warrior' Warfighting Experiment (AWE18), involving, among others, UK and US military services as well as industry.[205] Another product is the Skeeter, "disruptive drone technology" developed with funding from the UK government's Defence Science and Technology Laboratory (Dstl).[206]

In March 2019 Animal Dynamics took over UK software developer **Accelerated Dynamics**, whose motto was "making robots smarter", building technology "to drive the 4th industrial revolution".[207] It has developed ADx autonomous flight-control software based on gaming principles, through which each system is controlled by a central computer running the artificial intelligence software. The merger of the two companies combines "the ADx system with the small, flapping Skeeter UAV [and] will allow it to be operated in a swarm configuration for defence applications plus farming and surveys".[208] Accelerated Dynamics describes its AD Platform v1.2 as "the world's first autonomous UAV software platform", with four levels of autonomy, including one where "the user is not involved in the decision-making process, the system decides and executes autonomously".[209] Such fully autonomous missions include inspection, mapping, and search and rescue.

In one of the most elaborate responses to our survey, Animal Dynamics states that "increasing levels of autonomy across all industries are inevitable as computational power increases and autonomous systems become more sophisticated and reliable. The uses to which this can be put are both beneficial and harmful, depending on the intent of the user".[210] CEO Caccia furthermore stresses that "under our company charter, and our relationship with Oxford University, we will not weaponize or provide 'kinetic' functionality to the products we make".[211] Also, he believes that governments should make legislation to prevent harmful uses. "Every new technology can be put to malicious use; autonomy is no exception. Halting the technical development of autonomy is futile, and would prevent the many beneficial outcomes of autonomy; however, legislating against harmful uses for autonomy is an urgent and necessary matter for government and the legislative framework to come to terms with, in the same way has it has come to terms with (to name a few) nuclear (fission weapons vs power generation), biochemistry (medicine vs nerve agents), and the Internet (access to information vs political manipulation and hacking)".[212]

Israeli company **Airobotics** responded to our survey stating that its "drone system has nothing to do with weapons and related industries". The company wrote that the survey is therefore not relevant for them and they did "not wish to take part in it".[213] Indeed, while its drones are described as "Fully Automatic - Programmable, self-deploying, landing and servicing - no operator required", they are advertised for industrial purposes, including inspection, surveying and mapping, security and emergency responses.[214] It claims it was granted the first certificate in the world to fly a fully automated drone with no human operator.[215]

It may have nothing to do with weapons directly, but Airobotics clearly has links with the military and security business. In 2017 the company announced its new Homeland Security and Defense division, as well as an initiative called 'Airobotics Safe Cities' to perform emergency services.[216] In that context it planned to focus more on border security, and in particular the US-Mexico border, with "flying patrol bots" giving guards the ability to decide on a course of action in certain situations.[217]

Interviewed by an Israeli tech zine, co-founder Rann Krauss draws the line at adding weapons to the drones. "We decided to draw the line at physical intervention. The drone can use a flashlight to light the scene but not shoot tear gas or live ammunition", he explained".[218] While drawing that line sounds clear, its response to our survey appears to ignore the fact that its close links with the military and paramilitary market demand a clear company policy that its products may not be used to attack people.

Founded in 1993, **Heron Systems** provides "leading-edge solutions for national security customers" and its mission is "to strengthen America's defense by providing innovative laboratory testing and simulation solutions".[219] For example, MACE is its "lightweight robotic hardware/software architecture enabling cooperative communications and planning operations between autonomous systems [...] Designed to deploy on a [...] computer that allows for "plug-and-play" swarm capabilities".[220]

**Percepto** offers the Sparrow, an autonomous "drone-in-the-box solution [...] powered by computer vision and AI, [providing] constant aerial visual insights to help you optimise your security and business operations".[221] "The Sparrow autonomous drone deploys from its base station to perform on-demand or prescheduled missions, automating critical data collection and analysis processes and providing real-time visibility of site conditions".[222] "Security teams benefit from additional patrols done by the drone without the need for a pilot. These patrols leverage cutting-edge analytics to detect or track humans and cars both for supervision and intruder detection".[223] "On-board machine vision automatically alerts personnel of potential threats".[224]

While uses in the area of military and border security operations appear logical, Percepto focuses explicitly on industrial applications. Replying to our survey request, Percepto said: "We appreciate the opportunity to participate in this survey, however, since we develop solutions to the industrial markets, addressing security, safety and operational needs, the topic of lethal weapon[s] is completely out of the scope of our work. We therefore choose to opt out this survey".[225]

**"Shield AI"**s mission is to protect service members and innocent civilians with artificially intelligent systems".[226] It makes systems based on Hivemind, AI that enables robots "to learn from their experiences".[227]

San Diego based Shield AI was set up in 2015 and its first product, Nova, is a "combat proven", Hivemind-powered robot that autonomously searches buildings while simultaneously streaming video and generating maps.[228] "Nova enables fully autonomous access and exploration of buildings, dense urban environments and GPS-absent areas to produce better mission outcomes and to reduce risk to operators. Nova flies itself and works in the day and in darkness".

Shield AI works with the Pentagon and the Department of Homeland Security "to enable fully autonomous unmanned systems that dramatically reduce risk and enhance situational awareness in the most dangerous situations".[229]

## SWARMING DRONES

Some companies take UAVs a step further and work on swarm technologies. Swarm technology "allows a group of UAVs to complete an objective whilst coordinating with one another",[230] where "the basic idea of a drone swarm is that its machines are able to make decisions among themselves".[231] While of course there are numerous civilian applications conceivable that may be very useful and beneficial, experts warn about their application in attack roles.

There are particular fears regarding autonomous human-out-of-the-loop swarms, where operations could happen at speeds inconceivable to humans, risking rapid conflict escalation and mass casualties, whether intended or not, and great difficulty in deciding who was the perpetrator. A fictitious video called 'Slaughterbots', made by the Future of Life Institute in late 2017, clearly visualised that potential threat.[232]
An EU-funded border control project Roborder,[233] that plans to deploy "common technology", but "what would be groundbreaking for the companies involved is a functional system that allows

swarms of drones to operate autonomously and in unison to reliably identify targets".[234]
"The system will only identify that 'this object is human', nothing more", according to the programme manager, though adding facial recognition would be "technologically possible".[235] In this context, robotics professor Noel Sharkey argues that there is a thin dividing line between using robots to monitor a border and using them to enforce one. He worries about the implications of developing autonomous systems to patrol borders, including how the system could be used by a country coping with a large influx of people.[236]

The UK company **Blue Bear Systems** undertakes research into all aspects of unmanned systems and autonomy, including big data, artificial intelligence, electronic warfare and swarming systems.[237] It is at the forefront of "task tailored configurable autonomy", according to the company. "We have developed next generation capability in applying autonomy to vehicles, systems and even data. Our autonomy technology can be developed to work with our customers systems and we provide everything from low level control algorithms to systems of systems autonomy. […] We work with air, maritime and land systems, and our technology is equally applicable to military and civilian systems".[238]

In March 2019 a consortium headed by Blue Bear was awarded GBP 2.5 million for the development of drone swarm technology for the UK Ministry of Defence (MoD). The funding will be used to move into the final development stages for around 20 unmanned aerials systems and will seek "to establish a more 'self-sufficient' UAS swarm, providing the military with the ability to operate in increasingly complex and contested environments. Effective Human Machine Teaming will remain at the core of this research to ensure that the human remains firmly in control of the system".[239] The consortium also includes IQHQ, Airbus, Plextex and the University of Durham.

Set up in 2016, **Corenova Technologies** ("military-grade solutions to secure autonomous operations") offers HiveDefense, "an evolving swarm of self-learning bots that collaborate with blockchain to sense and respond to real-time events on digital and physical infrastructure".[240] It aims to focus on "maximising collaboration between machines and their human operators, leveraging automation to secure and distribute actionable intelligence in real-time".[241]
Corenova also works with DARPA on OFFSET,[242] which is evaluating tools and methods to conduct missions where "robotic systems will assume collaborative missions without human control, helping other robots [perform] complete missions autonomously".[243] OFFSET will be "using swarms compromising upwards of 250 unmanned aircraft systems (UASs) and/or unmanned ground systems (UGSs) to accomplish diverse missions in complex urban environments".[244]

## COUNTER-DRONE SYSTEMS

In the fast-growing area of counter-drone systems, numerous companies advertise their products as autonomous. Whereas for most this refers to navigational capabilities, some claim to have autonomous attack capabilities.

Most companies in this area focus on the protection of key public infrastructure and mass events, as well as military targets, against potential drone threats. The major disruption of operations at Gatwick airport in December 2018 due to the presence of an unidentified drone over the area and the subsequent issues in attempting to identify the origin of the drone were illustrative of the current lack of trustworthy, commercially available counter-drone technologies. On the other hand, there is no lack of companies claiming to develop the ultimate solution for dealing with 'unauthorised' drones.
The Canadian company **AerialX** is developing the DroneBullet, a kamikaze drone that looks like a miniature missile while having the capability of a quadcopter.[245] It covers a maximum three kilometre range and has an operational endurance of ten minutes. Weighing 910g, the system can achieve attack speeds of up to 200 km/h and a dive attack speed of up to 300 km/h "to optimise the effector's hit-to-kill capabilities".[246] DroneBullet's key feature "is its 'machine vision target system': an artificial intelligence (AI)-led capability that enables the system to autonomously identify, track and engage (or not engage) an approved target set"; its camera can also see at night.[247] It is programmed to only engage specifically approved drones based on characteristics such as multi-rotor/fixed-wing, model or colour, analysing a "target against a built-in threat library and, based on the AI algorithm confidence level, it will make a decision. If this is what it is looking for it will continue with the attack; if not, it will abort", according to AerialX chief executive Noam Kenig. Although DroneBullet is not controlled remotely, it has a ground station that activates and communicates with the system. "The ground station supplies basic information to the effector: 'attack', 'abort', target location, etc., but DroneBullet is essentially a fire-and-forget solution. Even if you lose communication, the unit will still continue with the mission; the moment the system is launched it proceeds independently to the engagement," said Kenig.[248] It is not difficult to see how such fire-and-forget technology could work with a different target library against other types of targets. Indeed AerialX is working to modify the weapon "for a warhead-equipped loitering munition solution".[249]

**Citadel Defense**—a "Silicon Valley success story"—was founded in 2016.[250] "Citadel protects soldiers from drone attacks and surveillance in enemy combat".[251] "Through autonomy, proprietary machine learning and artificial intelligence capabilities, Citadel Defense creates a force multiplier for Warfighters that enables them to get more done with the same or fewer resources. With the deployment of Citadel's technology, U.S. Special Operations Forces gain a modernized capability designed and developed to evolve with the pace of the growing threat".[252] The US Air Force recently contracted Citadel to provide solutions that can defeat weaponised drones and swarms.[253]
Citadel Defense produces a counter-drone system named Titan: "designed to operate autonomously using artificial intelligence. This allows operators to focus on their mission, not the equipment".[254]
Its Hunter Algorithm "is updated in weeks rather than months to address the new threat".[255]
Lastly, US company **Airspace Systems** "uses artificial intelligence and advanced robotics" for airspace security, including "long-range detection, instant identification, and autonomous mitigation – capture and safe removal of unauthorised or malicious drones. […] Airspace solutions provide operators with 3D situational awareness and actionable intelligence, enabling quick response".
"Co-developed and trusted by the US Department of Defense, the Airspace Interceptor is a fully autonomous system that captures unauthorised drones and then delivers them to a safe place to prevent damage to people or property".[256]

In March 2018, Airspace reported that it had raised USD 20 million to "guard critical infrastructure, public spaces and the military from enemy drones. […] The company utilises AI, machine vision and deep-learning neural networks to defend against the most complex drone threats faced by public event venues, military personnel and law enforcement agencies".[257] "We're leveraging the bleeding edge of artificial intelligence, computer vision, high-speed robotics and neural networks to create something like a firewall in the sky," said co-founder and CEO Banga, "We're building the complete drone security system that lets the good drones in and keeps the bad ones out".[258]

## 3.7 Ground Robots

Of more recent date is the breakthrough of increasingly autonomous robotic systems that operate on land. One tech company famous for having combined military and civilian products is iRobot, developer of both the Roomba robotic vacuum cleaner and PackBot, the robot that cleared improvised explosive devices (IEDs) in Iraq, Afghanistan and elsewhere.[259] In 2016, iRobot sold off its military activities.[260]

Another big name in robotics is Japanese telecom conglomerate **SoftBank**, which is known to invest large sums in new technology. Its USD 100 billion Vision Fund, in partnership with Saudi Arabia's sovereign wealth fund, is part of the Saudi strategy for diversifying away from oil. Vision Fund invests in AI tech companies, including BrainCorp, NVIDIA and Slack Technologies, and in solar power and electric vehicles.[261] Softbank also owns some 30 per cent of China's Alibaba.

SoftBank Robotics is best known for its humanoid Pepper robot. In 2017 it bought Boston Dynamics from Google.[262] Boston Dynamics was long closely connected to DARPA, as it pioneered techniques for helping robots manoeuvre in real-world environments.[263] In the same deal, SoftBank also took over the Japanese company Schaft, which won the 2013 robotics challenge organised by DARPA (see below).

In response to our survey, SoftBank states that their philosophy is "to use the Information Revolution to contribute to the well-being of people and society. As such, we do not have a weapons business and have no intention to develop technologies that could be used for military purposes".[264]

Several other surveyed companies have developed robotic systems that are aimed in particular at military markets. For instance, **Roboteam** was launched in 2009 by two former commanders with "access to the Israel Defense Forces as our backyard for testing".[265] It soon saw its turnover ballooning, with strong sales of ground robotic systems to the US military.[266] In 2014, it was labelled a "priority provider to the Pentagon's Combating Terrorism Technical Support Office (CTTSO)". Its Micro Tactical Ground Robot (MTGR) was ordered for Israel's anti-tunnel operations during the 2014 Gaza war, also known as Operation Protective Edge.[267] Up to 250 MTGRs were ordered a year later by the US Air Force under a USD 25 million contract.[268]

In 2018 it presented its Artificial Intelligence Control Unit (AI-CU, pronounced "IQ"), bringing autonomous navigation, facial recognition and other AI-enabled capabilities to the control and operation of unmanned systems and payloads.[269] AI-CU enables operators to control numerous platforms and payloads simultaneously, based on a multi-robot operator control unit. "The AI-CU will revolutionize the way soldiers are able to execute their mission objectives safely and successfully", according to self-confident Roboteam CEO Shahar Abuhazira.

Roboteam came under the spotlight last year for its links with Chinese investment firm FengHe Fund Management, which appears to have been bad publicity affecting its chances of winning a series of US Army robotics contracts as well as beating its main competitor, Endeavour Robotics (now FLIR).[270] Other customers include the Thai and Swiss ministries of defence.[271]

Another Israeli robotics company mainly dealing with the defence and security market is **General Robotics**, set up in 2009 by Ehud Gal, with a career in the defence ministry's R&D authority. General Robotics supplies "advanced robotics systems to counter-terrorist units worldwide"; many are designed to be used in 'urban warfare' contexts.[272]

Their products include the Pitbull, an urban warfare remote weapon system that has an "embedded 'Anti-Drone Track & Shoot' real time algorithm" and "smart sensors such as hostile fire source detector and radar".[273] Best known is Dogo, said to be "the world's first inherently armed tactical combat robot".[274] Dogo's movements and weaponry, however, are controlled by a person using a hand-held, tablet-like device, rather than artificial intelligence, according to the company.[275]

In response to our survey request, General Robotics CEO Shahar Gal shows he is clearly aware of the discussion around robotics and AI. He writes: "Our position is not to allow lethal autonomous weapons without human supervision and human final active decision. […] In general, our systems are designed to provide real-time high quality information and to present it to a trained human operator in an intuitive manner; this insures better decision making by the human and thereby better results with less casualties".[276]

### AUTONOMOUS DRIVING

Over the past decade, huge investments have been made in autonomous driving technology, combining "sensors and software to control, navigate, and drive the vehicle".[277] The software can include object detection and recognition algorithms, and self-driving systems often "create and maintain an internal map of their surroundings, based on a wide array of sensors, like radar".[278]

Much like self-driving cars, military robotic vehicles can navigate without the "fatigue, distractions and other human fallibilities". Yet at the same time, increasingly intelligent machines may interpret the world differently from humans, as accidents with self-driving cars have shown.[279]

Much technological progress in this area was initially fostered with military money and through the DARPA 'challenges' that have been held since 2004 to test (human-supervised) autonomous ground robots capable of executing complex tasks.[280] Today, more and more R&D in this sector is driven by the commercial industry—but often still linked to the military industry.[281] And clearly, military programmes will increasingly use consumer-based technology for warfighting applications.
The Israeli company **Innoviz** makes laser-based radar for cars. "Its sensors allow remote 3D scanning and provide a high-definition image of a vehicle's surrounding".[282] The company was founded by former members of the elite technological unit of the Israeli Defense Forces, but currently does not appear to be engaged in military work.[283]

Another Israeli company in this area is **Arbe Robotics**, with its motto "bringing the power of radar to autonomous driving".[284] Arbe Robotics started off in the military and homeland security, before moving to cars.[285] In response to our survey the company mentions that it "will sign agreements with customers that would confirm that they are not using our technology for military use".[286]

The French company **Dibotics**—"make sense out of sensor data"—also works on autonomous navigation.[287] Their applications include airborne mapping using lidar and infrastructure surveillance with drones. Dibotics is supported by 'Generate', a programme for French defence start-ups initiated by the industry umbrella organisation GICAT.[288]

Dibotics founder and CEO Raul Bravo signed the Future of Life Institute's 2017 open letter to the UN,[289] but the company did not answer requests to participate in our survey.

# 4. Conclusions & Recommendations

This report has provided an overview of developments in the tech sector that are relevant in the context of lethal autonomous weapons that can select and attack targets without meaningful human control. The emergence of such weapons will have an enormous effect on the way war is conducted. İt has been called the third revolution in warfare, after gunpowder and the atomic bomb.

Significantly, as part of an imminent arms race to develop increasingly autonomous weapons, states rely on and push to involve the tech sector in those efforts. While digital technology, especially artificial intelligence, can be beneficial in many ways, in order to realize those benefits for humanity, countless AI and robotics experts have warned that the technology should not be applied to develop lethal autonomous weapons.

Large numbers of leading figures working in the tech sector, including from US giants such as Apple, Facebook, IBM, Intel and Microsoft, endorsed a 2015 open letter saying that "a military AI arms race is a bad idea, and should be prevented by a ban on offensive autonomous weapons beyond meaningful human control".

Yet these same companies have so far themselves shown limited willingness to commit to public policies that ensure their technology will not be used in the development of lethal autonomous weapons. Countless other big tech companies – including Chinese counterparts such as Alibaba, Baidu, Megvii, Sensetime and Tencent - have so far also remained silent.

Tech workers, for example at Microsoft, have started to resist working on weapons development projects, saying that they "don't believe what we build should be used for waging war" and that they worked there in the hope of empowering "every person on the planet to achieve more, not with the intent of ending lives and enhancing lethality".

Such resistance has proven successful in some cases, most notably with Google, who subsequently withdrew from the Pentagon's infamous project Maven and developed an AI policy to not design or deploy AI in "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people".

Tech companies need to become aware that unless they take measures, their technology could contribute to the development of lethal autonomous weapons. They must also be aware that engagement, or perceived engagement, in developing lethal autonomous weapons systems would likely be bad for business, could result in reputational damage and potentially impair their ability to attract and retain top tech talent. Setting up clear, publicly-available policies is an essential strategy to prevent this from happening.

As Canadian company Clearpath Robotics has said: "Clearpath continues to believe that the proliferation of lethal autonomous weapon systems remains a clear and present danger to the citizens of every country in the world. No nation will be safe, no matter how powerful".[290] Clearpath is among 247 companies and organisations that have signed a pledge not to engage in any work related to lethal autonomous weapons.

In addition, as part of the survey for this report, Animal Dynamics (UK), Arbe Robotics (Israel), Google (US), Softbank (Japan) and VisionLabs (Russia) have explained how they ensure their technologies will not be used for the development or production of autonomous weapons.

However, it is deeply concerning that other tech companies, especially those working on military contracts, do not currently have any public policy to ensure their work is not contributing to lethal autonomous weapons. Besides Amazon and Microsoft, mentioned above, AerialX (Canada), Anduril, Clarifai and Palantir (all US) emerge in this report as working on technologies relevant to increasingly autonomous weapons and did not reply in any meaningful way to our survey.

## Recommendations

There are concrete steps companies can take to prevent their products contributing to the development and production of lethal autonomous weapons.

- Commit publicly to not contribute to the development of lethal autonomous weapons.[291]

- Establish a clear policy stating that the company will not contribute to the development or production of lethal autonomous weapon systems. This policy should include implementation measures such as:
  - Ensuring each new project is assessed by an ethics committee;
  - Assessing all technology the company develops and its potential uses and implications;
  - Adding a clause in contracts, especially in collaborations with ministries of defence and arms producers, stating that the technology developed may not be used in lethal autonomous weapon systems.

- Ensure employees are well informed about what they work on and allow open discussions on any related concerns.

# List of Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| AR | Augmented Reality |
| DARPA | Defense Advanced Research Projects Agency |
| DoD | Department of Defense (US) |
| JEDI | Joint Enterprise Defense Infrastructure |
| LAWS | Lethal Autonomous Weapon Systems |
| ML | Machine Learning |
| MoD | Ministry of Defence |
| NATO | North Atlantic Treaty Organisation |
| UAS | Unmanned Aerial System |
| UAV | Unmanned Aerial Vehicle |
| UGV | Unmanned Ground Vehicle |
| UN | United Nations |
| VR | Virtual Reality |



# Annex: Survey Questions

All companies surveyed and included in the table in chapter 3 were asked four questions:

## Survey questions

When we mention 'lethal autonomous weapons' below we define them as 'weapon systems that can autonomously select and attack targets'.

1. Are you aware of the international debate regarding lethal autonomous weapons systems and the concerns raised regarding these weapons? Does that debate influence your work?

2. Does your company have a position on lethal autonomous weapons? If yes, what is that position? If no, why not?

3. Does your company have a formal policy to ensure your work and the technology you develop do not contribute to the development of lethal autonomous weapons? Does your company adhere to external guidelines regarding this? If so, can you share this policy and/or guidelines? If not, why not?

4. Is your company currently researching and/or developing lethal autonomous weapons systems? (Yes/No/Prefer not to answer)

# Notes

1 R. Vinuesa et al, 'The role of artificial intelligence in achieving the Sustainable Development Goals', 2019, https://arxiv.org/ftp/arxiv/papers/1905/1905.00501.pdf.

2 'Letter to Google CEO', The New York Times, https://static01.nyt.com/files/2018/technology/googleletter.pdf.

3 Google email, received 21 May 2019.

4 Employees of Microsoft, 'An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI', Medium, 12 October 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132

5 Meghan Hennessey, 'Clearpath Robotics Takes Stance Against 'Killer Robots'', Clearpath Robotics, 13 August 2014, https://www.clearpathrobotics.com/blog/2014/08/clearpath-takes-stance-against-killer-robots/

6 Within the UN and elsewhere, lethal autonomous weapon systems are often referred to as LAWS or as fully autonomous weapon systems, and more popularly as killer robots. In this report we will use the terms 'lethal autonomous weapons' and 'autonomous weapons' interchangeably. For more information on the UN process, see: https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument. For a brief general introduction to this topic, see: https://www.paxforpeace.nl/media/files/pax-booklet-killer-robots-what-are-they-and-what-are-the-concerns.pdf

7 Future of Life Institute, 'Autonomous Weapons: An Open Letter From AI & Robotics Researchers', 28 July 2015, https://futureoflife.org/open-letter-autonomous-weapons/.

8 See amongst others: Peter Asaro, 'On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making', International Review of the Red Cross, No. 886, 2012; Human Rights Watch, 'Heed the Call A Moral and Legal Imperative to Ban Killer Robots', August 2018 ; Heather Roff, 'Killing in War: Responsibility, Liability and Lethal Autonomous Robots', 2014; Robert Sparrow, "Killer robots", in Journal of Applied Philosophy, 24(1), 2007.

9 Bonnie Docherty, 'Mind the Gap: the Lack of Accountability for Killer Robots', Human Rights Watch, 9 April 2015, https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots. Thomas Chengeta, 'Accountability Gap, Autonomous Weapon Systems and Modes of Responsibility in International Law', SSRN, 30 September 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755211.

10 Paul Scharre, 'Killer Apps: The Real Dangers of an AI Arms Race', Foreign Affairs, May/June 2019, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps

11 Stuart Russell, 'The new weapons of mass destruction?', The Security Times, February 2018, https://www.securityconference.de/fileadmin/MSC_/2018/Dokumente/Security_Times_Feb2018.pdf.

12 Ian Sample, 'Ban on killer robots urgently needed, say scientists', The Guardian, 13 November 2017, https://www.theguardian.com/science/2017/nov/13/ban-on-killer-robots-urgently-needed-say-scientists.

13 China states that its call is to ban the use of fully autonomous weapons, but not their development or production

14 'Killer Robots – What are they and what are the concerns?', PAX, March 2019, https://www.paxforpeace.nl/media/files/pax-booklet-killer-robots-what-are-they-and-what-are-the-concerns.pdf,

15 Ian Sample, 'Ban on killer robots urgently needed, say scientists', The Guardian, 13 November 2017, https://www.theguardian.com/science/2017/nov/13/ban-on-killer-robots-urgently-needed-say-scientists,

16 Meghan Hennessey, 'Clearpath Robotics Takes Stance Against 'Killer Robots'', Clearpath Robotics, 13 August 2014, https://www.clearpathrobotics.com/blog/2014/08/clearpath-takes-stance-against-killer-robots/,

17 Ibid.

18 Future of Life Institute, 'Autonomous Weapons: An Open Letter From AI & Robotics Researchers', 28 July 2015, https://futureoflife.org/open-letter-autonomous-weapons/.

19 Future of Life Institute, 'Killer robots: World's top AI and robotics companies urge United Nations to ban lethal autonomous weapons', 20 August 2017, https://futureoflife.org/2017/08/20/killer-robots-worlds-top-ai-robotics-companies-urge-united-nations-ban-lethal-autonomous-weapons/,

20 Ariel Conn, 'Leaders of Top Robotics and AI Companies Call for Ban on Killer Robots', Future of Life Institute, 20 August 2017, https://futureoflife.org/2017/08/20/leaders-top-robotics-ai-companies-call-ban-killer-robots/,

21 A.M. Turing Award, 'Geoffrey Hinton and Yann LeCun to deliver Turing lecture at FCRC 2019', June 2019, https://amturing.acm.org/

22 The Future of Life, 'Lethal autonomous weapons pledge', 2018, https://futureoflife.org/lethal-autonomous-weapons-pledge/ and Ariel Conn, 'AI Companies, Researchers, Engineers, Scientists, Entrepreneurs, and Others Sign Pledge Promising Not to Develop Lethal Autonomous Weapons', Future of Life Institute, 18 July 2018, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/.

23 BDI, 'Künstliche Intelligenz in Sicherheit und Verteidigung', 15 January 2019, https://bdi.eu/publikation/news/kuenstliche-intelligenz-in-sicherheit-und-verteidigung (translation by author).

24 'Letter to Google CEO', The New York Times, https://static01.nyt.com/files/2018/technology/googleletter.pdf.

25 Campaign to Stop Killer Robots, 'Google, other companies must endorse ban', 16 May 2018, https://www.stopkillerrobots.org/2018/05/google/ and Cheryl Pellerin, 'Project Maven to Deploy Computer Algorithms to War Zone by Year's End', DoD News, 21 July 2017, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

26 'Letter to Google CEO', The New York Times, https://static01.nyt.com/files/2018/technology/googleletter.pdf.

27 Amr Gaber speaking at a side-event at the CCW on 28 August 2018.

28 Google, 'Artificial Intelligence at Google: Our Principles', https://ai.google/principles/.

29 Google email, received 21 May 2019.

30 Kate Conger and Cade Metz, 'Tech Workers Now Want to Know: What Are We Building This For?', The New York Times, 7 October 2018, https://www.nytimes.com/2018/10/07/technology/tech-workers-ask-censorship-surveillance.html.

31 Jasmine Garsd, 'When Technology Can Be Used To Build Weapons, Some Workers Take A Stand', NPR, 13 May 2019, https://www.npr.org/2019/05/13/722909218/when-technology-can-be-used-to-build-weapons-some-workers-take-a-stand?t=1558000179454.

32 Matthew Zeiler, 'Why We're Part of Project Maven', Clarifai, 13 June 2018, https://blog.clarifai.com/why-were-part-of-project-maven.

33 Jasmine Garsd, 'When Technology Can Be Used to Build Weapons, Some Workers Take A Stand', NPR, 13 May 2019, https://www.npr.org/2019/05/13/722909218/when-technology-can-be-used-to-build-weapons-some-workers-take-a-stand?t=1558429685106.

34 Ibid.

35 Kyle Wiggers , 'Andrew Yang: The U.S. government is 24 years behind on tech', Venture Beat, 21 May 2019, https://venturebeat.com/2019/05/21/andrew-yang-the-u-s-government-is-24-years-behind-on-tech/.

36 Clarifai email, received via Trailrunner International, 24 April 2019. Trailrunner also replied on behalf of Anduril, another company involved in Project Maven.

37 Microsoft is also working on the Azure "secret-level cloud" for the US government; see e.g.: Jessie Bur, 'Microsoft progresses on secret cloud ahead of JEDI decision', Federal Times, 17 April 2019, https://www.federaltimes.com/govcon/2019/04/17/microsoft-progresses-on-secret-cloud-ahead-of-jedi-decision/.

38 Employees of Microsoft, 'An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI', Medium, 12 October 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132.

39 Ibid.

40 Colin Lecher, 'Microsoft workers' letter demands company drop Army HoloLens contract', The Verge, 22 February 2019, https://www.theverge.com/2019/2/22/18236116/microsoft-hololens-army-contract-workers-letter.

41 Microsoft Workers 4 Good, Twitter status, 22 February 2019, https://twitter.com/MsWorkers4/status/1099066343523930112.

42 Colin Lecher, 'Microsoft workers' letter demands company drop Army HoloLens contract', The Verge, 22 February 2019, https://www.theverge.com/2019/2/22/18236116/microsoft-hololens-army-contract-workers-letter.

43 Microsoft Workers 4 Good, Twitter status, 22 February 2019, https://twitter.com/MsWorkers4/status/1099066343523930112.

44 Eric Horvitz email, received 9 August 2019.

45 Brad Smith, 'Technology and the US military', Microsoft, 26 October 2018, https://blogs.microsoft.com/on-the-issues/2018/10/26/technology-and-the-us-military/.

46 Microsoft Corporate Blogs, 'Brad Smith takes his call for a Digital Geneva Convention to the United Nations', 9 November 2017, https://blogs.microsoft.com/on-the-issues/2017/11/09/brad-smith-takes-call-digital-geneva-convention-united-nations/

47 Kate Conger, 'Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program', Gizmodo, 1 June 2018, https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620.

48 Kevin Roose, 'Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts', The New York Times, 4 March 2019, https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html.

49 Sam Shead, 'U.K. Tech Staff Quit Over Work On 'Harmful' AI Projects', Forbes, 13 May 2019, https://www.forbes.com/sites/samshead/2019/05/13/uk-tech-staff-quit-over-work-on--harmful-ai-projects/#140b9c6f4df5.

50 Ian Sample, 'Ban on killer robots urgently needed, say scientists', The Guardian, 13 November 2017, https://www.theguardian.com/science/2017/nov/13/ban-on-killer-robots-urgently-needed-say-scientists.

51 IEEE, 'The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems', visited 7 June 2019, https://standards.ieee.org/industry-connections/ec/autonomous-systems.html.

52 IEEE, 'Reframing Autonomous Weapons Systems V2', https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_reframing_autonomous_weapons_v2.pdf

53 IBM, 'Every day ethics', 2019 https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf

Microsoft, 'The Future Computed'2018, https://blogs.microsoft.com/uploads/2018/02/The-Future-Computed_2.8.18.pdf

54 Partnership on AI, 'Tenets', https://www.partnershiponai.org/tenets/.

55 University of Montreal, 'The Montreal Declaration for a Responsible Development of Artificial Intelligence: a participatory process' , November 2017, https://www.montrealdeclaration-responsibleai.com/the-declaration

56 Future of Life Institute, 'Asilomar AI principles', January 2017, https://futureoflife.org/ai-principles/

57 See e.g. Ariel Conn, 'AI Companies, Researchers, Engineers, Scientists, Entrepreneurs, and Others Sign Pledge Promising Not to Develop Lethal Autonomous Weapons', Future of Life Institute, 18 July 2018, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/.

58 Campaign to Stop Killer Robots, '10 Ways for Tech Workers to Get Involved', 12 June 2019, https://www.stopkillerrobots.org/2019/06/10-ways-for-tech-workers-to-get-involved-2/.

59 Davey Winder, 'Ten amazing DARPA inventions', 29 March 2016, https://www.alphr.com/features/373546/10-brilliant-darpa-inventions/page/0/2.

60 In 2009, Peter Singer estimated that the "U.S. military funds as much as 80 percent of all AI research in the United States" ('Wired for War', Penguin Press, p.78).

61 See e.g. Scott Alexander, 'Follow the leader – US Army unmanned ground vehicle programmes', Jane's Defence Weekly, 17 April 2019.

62 Peter Burt, 'Off the leash – the development of autonomous military drones in the UK', Drone Wars UK, November 2018, https://dronewars.net/wp-content/uploads/2018/11/dw-leash-web.pdf.

63 Melanie Rovery, 'AI: The effects on future land forces', Jane's International Defence Review, June 2019.

64 See e.g. this UK Ministry of Defence's concept note on "the challenges and opportunities of robotic and artificial intelligence (AI) technologies and how we can achieve military advantage through human-machine teams": https://www.gov.uk/government/publications/human-machine-teaming-jcn-118 or this MITRE/US Air Force Laboratory study: https://www.mitre.org/sites/default/files/publications/pr-17-4208-human-machine-teaming-systems-engineering-guide.pdf.

65 Peter Burt, 'Off the leash – the development of autonomous military drones in the UK', Drone Wars UK, November 2018, https://dronewars.net/wp-content/uploads/2018/11/dw-leash-web.pdf.

66 Some of the big companies may appear at more than one place in the report, as they work on multiple relevant technologies.

67 Other multi-billion businesses feature in other parts of the report.

68 Jordan Novet and Amanda Macias, 'IBM and Oracle are out of the running for $10 billion government cloud contract', 11 April 2019, https://www.cnbc.com/2019/04/11/amazon-microsoft-finalists-for-10-billion-government-cloud-contract.html.

69 Therese Poletti, 'Opinion: The JEDI war: Amazon, Oracle and IBM battle in mysterious world of military contracts', 8 January 2019, https://www.marketwatch.com/story/the-jedi-war-amazon-oracle-and-ibm-battle-in-mysterious-world-of-military-contracts-2019-01-07.

70 Employees of Microsoft, 'An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI', Medium, 12 October 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132.

71 Mark Bergen, 'Inside Google, a Debate Rages: Should It Sell Artificial Intelligence to the Military?', Bloomberg, 14 May 2018, https://www.bloomberg.com/amp/news/articles/2018-05-14/inside-google-a-debate-rages-should-it-sell-artificial-intelligence-to-the-military.

72 Frank Konkel, 'Microsoft, Amazon CEOs Stand By Defense Work After Google Bails on JEDI', NextGov.com, 15 October 2018, https://www.nextgov.com/it-modernization/2018/10/microsoft-amazon-ceos-standby-defense-work-after-google-bails-jedi/152047/.

73 Frank Konkel, 'Microsoft, Amazon CEOs Stand By Defense Work After Google Bails on JEDI', NextGov.com, 15 October 2018, https://www.nextgov.com/it-modernization/2018/10/microsoft-amazon-ceos-standby-defense-work-after-google-bails-jedi/152047/.

74 Naomi Nix, 'Google Drops Out of Pentagon's $10 Billion Cloud Competition', Bloomberg, 8 October 2018, https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition.

75 Employees of Microsoft, 'An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI', Medium, 12 October 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132.

76 Wikipedia, 'Oracle Corporation', https://en.wikipedia.org/wiki/Oracle_Corporation

77 Oracle, 'Artificial Intelligence', https://www.oracle.com/artificial-intelligence/.

78 Oracle, 'The Complete Cloud for Civilian and Defense Agencies', https://www.oracle.com/industries/public-sector/defense.html.

79 Rebecca Hill, 'Oracle throws toys out pram again, tells US claims court: Competing for Pentagon cloud contract isn't fair!', 15 February 2019, https://www.theregister.co.uk/2019/02/15/oracle_seeks_to_stop_pentagon_jedi/.

80 Bernard Marr, 'The Amazing Ways Chinese Tech Giant Alibaba Uses Artificial Intelligence and Machine Learning', Forbes, 23 July 2018, https://www.forbes.com/sites/bernardmarr/2018/07/23/the-amazing-ways-chinese-tech-giant-alibaba-uses-artificial-intelligence-and-machine-learning/.



81 Bernard Marr, 'How Chinese Internet Giant Baidu Uses Artificial Intelligence and Machine Learning', 23 July 2018, https://www.forbes.com/sites/bernardmarr/2018/07/06/how-chinese-internet-giant-baidu-uses-artificial-intelligence-and-machine-learning/#5fd1cb362d55.

82 AI Multiple (blog),'15 Examples on Baidu's Lead in Global AI Race [2019 update]', 4 January 2019, https://blog.aimultiple.com/baidu/.

83 Theodore Schleifer, 'Silicon Valley is awash in Chinese and Saudi cash — and no one is paying attention (except Trump)', Vox, 1 May 2019, https://www.vox.com/recode/2019/5/1/18511540/silicon-valley-foreign-money-china-saudi-arabia-cfius-firrma-geopolitics-venture-capital.

84 IISS, 'China's pursuit of advanced dual-use technologies', 18 December 2018, https://www.iiss.org/blogs/analysis/2018/12/emerging-technology-dominance and Elsa B. Kania, 'China's AI Giants Can't Say No to the Party, 2 August 2018, https://foreignpolicy.com/2018/08/02/chinas-ai-giants-cant-say-no-to-the-party/.

85 Elsa Kania, 'China's AI Agenda Advances', The Diplomat, 14 February 2018, https://thediplomat.com/2018/02/chinas-ai-agenda-advances/.

86 Bernard Marr, 'The Amazing Ways Chinese Tech Giant Alibaba Uses Artificial Intelligence and Machine Learning', Forbes, 23 July 2018, https://www.forbes.com/sites/bernardmarr/2018/07/23/the-amazing-ways-chinese-tech-giant-alibaba-uses-artificial-intelligence-and-machine-learning/.

87 Kane Wu and Julie Zhu, 'China's AI start-up Megvii raising $500 million at $3.5 billion valuation: sources', Reuters, 10 December 2018. https://www.reuters.com/article/us-megvii-fundraising-idUSKBN1O90AV.

88 Anita Balakrishnan, 'Jack Ma: World leaders must make 'hard choices' or the next 30 years will be painful', CNBC, 21 June 2017, https://www.cnbc.com/2017/06/21/alibabas-jack-ma-says-people-will-work-four-hours-a-day-in-30-years.html

89 Dean Takahashi, 'Tencent acquires Swedish game studio Sharkmob', Venturebeat, 21 May 2019, https://venturebeat.com/2019/05/21/tencent-acquires-swedish-game-studio-sharkmob/.

90 Synced, 'Tencent's New Medical AI Lab Targets Parkinson's', Medium, 8 December 2018, https://medium.com/syncedreview/tencents-new-medical-ai-lab-targets-parkinson-s-715c5a1b68f2.

91 Bernard Marr, 'Artificial Intelligence (AI) In China: The Amazing Ways Tencent Is Driving It's Adoption', 4 June 2018, https://www.forbes.com/sites/bernardmarr/2018/06/04/artificial-intelligence-ai-in-china-the-amazing-ways-tencent-is-driving-its-adoption/#2abe86a3479a.

92 Yuang Yang, 'China's Tencent pitches vision of artificial intelligence ethics', 1 May 2019, https://www.ft.com/content/f92abc38-6bb8-11e9-80c7-60ee53e6681d.

93 Samsung Research, 'Artificial Intelligence', https://research.samsung.com/artificial-intelligence.

94 Samsung email, received 11 April 2019.

95 Siemens, 'Artificial intelligence in industry: intelligent production', https://new.siemens.com/global/en/company/stories/industry/ai-in-industries.html.

96 John Keller, 'Siemens, Carnegie Mellon, and HRL pursue artificial intelligence to analyse images and text', 10 November 2013, https://www.militaryaerospace.com/articles/2013/11/siemens-iarpa-krns.html.

97 Ibid.

98 Printed Electronics Now, 'DARPA Chooses PARC, Siemens, Georgia Institute of Technology, MSU to Transform Manufacturing, 30 June 2017, https://www.printedelectronicsnow.com/contents/view_breaking-news/2017-06-30/darpa-chooses-parc-siemens-georgia-institute-of-technology-msu-to-transform-manufacturing/?widget=trending

99 Siemens email, received reply, 1 July 2019 re to Marta Kosmyna (Campaign to Stop Killer Robots).

100 Don Clark, 'Hewlett Packard Enterprise to Acquire Supercomputer Pioneer Cray', The New York Times, 17 May 2019, https://www.nytimes.com/2019/05/17/technology/hp-enterprise-cray-supercomputers.html.

101 'China Extends Supercomputer Share on TOP500 List, US Dominates in Total Performance', TOP500.org press release, November 2018, https://www.top500.org/news/lists/2018/11/press-release/.

102 The concept of big data can be understood as "extremely large data sets that can be analysed computationally to reveal patterns, trends, and associations". Gerrard Cowan, 'Number crunching', Jane's Defence Weekly, 15 May 2019.

103 Karen Hao, 'The next AI explosion will be defined by the chips we build for it', MIT Technology Review, 26 March 2019, https://www.technologyreview.com/s/613202/the-next-ai-explosion-will-be-defined-by-the-chips-we-build-for-it/.

104 Gerrard Cowan, 'Number crunching', Jane's Defence Weekly, 15 May 2019.

105 Wylie Wong, 'IBM Research Wants to Have Next-Gen AI Chips Ready When Watson Needs Them', Data Center Knowledge, 15 February 2019, https://www.datacenterknowledge.com/machine-learning/ibm-research-wants-have-next-gen-ai-chips-ready-when-watson-needs-them.

106 IBM, 'AI Hardware Center', https://www.research.ibm.com/artificial-intelligence/ai-hardware-center/.

107 BM, 'Building stronger defense and intelligence', https://www.ibm.com/industries/government/defense-intelligence.

108 Computing, 'Sequoia', https://computation.llnl.gov/computers/sequoia and Computing, 'Sierra', https://computation.llnl.gov/computers/sierra.

109 'Getting them to battle—and back: how AI is transforming readiness and the way Marines are deployed', IBM, https://www.ibm.com/industries/federal/national-security/marine-corps-ai-readiness.

110 Future of Life, 'Resarch priorities for robust and beneficial artificial intelligence', https://futureoflife.org/ai-open-letter/ and Future of Life, 'Open letter signatories',

https://futureoflife.org/ai-open-letter-signatories/

111 Intel, 'Tools', https://www.intel.ai/tools/.

112 Intel, 'Government', https://www.intel.ai/government/#gs.8vhxru.

113 Intel, 'Intel Named to DARPA Project Focused on Machine Learning and Artificial Intelligence', https://newsroom.intel.com/news/intel-named-darpa-project-focused-machine-learning-artificial-intelligence/#gs.8boe2t.

114 WikiChip Fuse, 'Intel Opens AIB for DARPA's CHIPS Program as a Royalty-Free Interconnect Standard for Chiplet Architectures', https://fuse.wikichip.org/news/1520/intel-opens-aib-for-darpas-chips-program-as-a-royalty-free-interconnect-standard-for-chiplet-architectures/.

115 Hugh Griffith, 'Bargain hunters: military forces eye innovative COTS UAV solutions', Jane's International Defence Review, April 2018.

116 Bernard Marr, 'The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance', Forbes, 14 February 2018, https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/.

117 Andrew White, 'Ready player one', Jane's Defence Weekly, 15 May 2019.

118 Ibid.

119 Ibid.

120 Issie Lapowsky, 'Inside The Room Where Tech Actually Vies For Military Jobs', 12 March 2019, https://www.wired.com/story/inside-air-force-demo-day-tech-companies/.

121 Ibid.

122 Ibid.

123 Kevin Roose, 'Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts', The New York Times, 4 March 2019, https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html.

124 Palantir, 'Intelligence', https://www.palantir.com/solutions/intelligence/.

125 Patrick Howell O'Neill, 'The Marriage of Silicon Valley and the Pentagon Is Happening Whether You Like It or Not', Gizmodo, 27 March 2019, https://gizmodo.com/the-marriage-of-silicon-valley-and-the-pentagon-is-happ-1833605329.

126 Kate Fazzini and Amanda Macias, 'Peter Thiel's company Palantir just won a major Pentagon contract, beating out traditional military vendors', CNBC, 27 March 2019, https://www.cnbc.com/2019/03/27/palantir-in-multi-million-dollar-pentagon-deal-ipo-on-horizon.html.

127 Shane Harris, 'Palantir wins competition to build Army intelligence system', The Washington Post, 26 March 2019, https://www.washingtonpost.com/world/national-security/palantir-wins-competition-to-build-army-intelligence-system/2019/03/26/c6d62bf0-3927-11e9-aaae-69364b2ed137_story.html?utm_term=.0f0810f585c6; Dan Robitzski, 'The US Military Is Hiring Palantir to Build Battlefield AI', Futurism, 27 March 2019, https://futurism.com/army-palantir-battlefield-ai.

128 See for instance, Sebastian Moss, 'Palantir wins $800m Pentagon battlefield intelligence contract', Data Center Dynamics, 28 March 2019, https://www.datacenterdynamics.com/news/palantir-wins-800m-pentagon-battlefield-intelligence-contract/ and Kate Fazzini and Amanda Macias, 'Peter Thiel's company Palantir just won a major Pentagon contract, beating out traditional military vendors', CNBC, 27 March 2019, https://www.cnbc.com/2019/03/27/palantir-in-multi-million-dollar-pentagon-deal-ipo-on-horizon.html.

129 Kate Fazzini and Amanda Macias, 'Peter Thiel's company Palantir just won a major Pentagon contract, beating out traditional military vendors', CNBC, 27 March 2019, https://www.cnbc.com/2019/03/27/palantir-in-multi-million-dollar-pentagon-deal-ipo-on-horizon.html.

130 Anduril Industries, Twitter status, 17 May 2019, https://twitter.com/anduriltech/status/1129380561057976321; see also e.g. Foreign Affairs, Twitter Status, 3 May 2019, https://twitter.com/ForeignAffairs/status/1124163458084286465

131 Lee Fang, 'Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract', The Intercept, 9 March 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/.

132 Aaron Mehta, 'Cultural divide: Can the Pentagon crack Silicon Valley?', Defense News, 28 January 2019, https://www.defensenews.com/pentagon/2019/01/28/cultural-divide-can-the-pentagon-crack-silicon-valley/.

133 Anduril Industries, https://www.anduril.com/.

134 Anduril Industries, 'The Lattice Platform', https://www.anduril.com/lattice-ai.

135 Lee Fang, 'Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract', The Intercept, 9 March 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/.

136 Andrew Liptak, 'Palmer Luckey's company earned a contract for the Pentagon's Project Maven AI program', 10 March 2019, https://www.theverge.com/2019/3/10/18258553/palmer-luckey-anduril-industries-pentagon-project-maven-ai-program-vr.

137 Lee Fang, 'Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract', The Intercept, 9 March 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/.

138 Anduril email received via Trailrunner International, 23 April 2019. Trailrunner also replied on behalf of Clarifai, another company involved in Project Maven.



139 SparkCognition, https://www.sparkcognition.com/.

140 'Former Deputy Secretary of Defense Robert O. Work Joins SparkCognition Advisory Board', SparkCognition press release, 1 July 2019, https://www.prnewswire.com/news-releases/former-deputy-secretary-of-defense-robert-o-work-joins-sparkcognition-advisory-board-300878337.html.

141 Marcus Weisgerber, 'For Sale: Artificial Intelligence That Teaches Itself', Defense One, 6 July 2017, https://cdn.defenseone.com/b/defenseone/interstitial.html.

142 SparkCognition, 'Defense', https://www.sparkcognition.com/industry/defense/.

143 SparkCognition, 'SparkCognition and British Army to Collaborate to Advance Artificial Intelligence Applications for Defense', 4 October 2017, https://www.prnewswire.com/news-releases/sparkcognition-and-british-army-collaborate-to-advance-artificial-intelligence-applications-for-defense-300530037.html.

144 August Cole and Amir Husain, 'Putin Says Russia's New Weapons Can't Be Beat. With AI and Robotics, They Can.', Defense One, 13 March 2018, https://www.defenseone.com/ideas/2018/03/putin-says-russias-new-weapons-cant-be-beat-ai-and-robotics-they-can/146631/.

145 Ibid.

146 Amir Husain and August Cole, 'A New Industrial Base Is Taking Shape. Call It the Military-AI Complex', Defense One, 6 June 2019, https://www.defenseone.com/ideas/2019/06/new-industrial-base-taking-shape-call-it-military-ai-complex/157503/.

147 Sandra Erwin, 'Defense Technologists Divided Over Killer Robots', Real Clear Defense, 24 August 2017, https://www.realcleardefense.com/articles/2017/08/24/defense_technologists_divided_over_killer_robots_112133.html.

148 Ibid.

149 https://hivemapper.com/.

150 Lara Seligman, 'A Silicon Valley Start-Up That Loves the Pentagon', Foreign Policy, 26 September 2018, https://foreignpolicy.com/2018/09/26/a-silicon-valley-startup-that-loves-the-pentagon-hivemapper-dod-google/.

151 Ibid.

152 https://futureoflife.org/open-letter-autonomous-weapons-full-list/.

153 Hivemapper email, received 11 April 2019.

154 Issie Lapowsky, 'Inside The Room Where Tech Actually Vies For Military Jobs', Wired, 12 March 2019, https://www.wired.com/story/inside-air-force-demo-day-tech-companies/.

155 Army Technology, 'Montvieux engineers develop predictive cognitive control tool for MoD', 20 July 2018, https://www.army-technology.com/news/montvieux-engineers-develop-predictive-cognitive-control-tool-uk-mod/.

156 DASA, 'Next Generation Applied Artificial Intelligence, 17 January 2019, https://www.gov.uk/government/news/next-generation-applied-artificial-intelligence.

157 EarthCube, https://www.earthcube.eu/.

158 EarthCube, 'Defense', https://www.earthcube.eu/defense.

159 Idriss Mekrez, 'Earthcube: Innovation for Activity-based Intelligence', 18 December 2018, https://www.marklogic.com/blog/earthcube-innovation-for-activity-based-intelligence/.

160 Ibid.

161 Christina Mackenzie, 'Vendors showcase defense tech for France's new innovation agency', Defense News, 27 November 2018, https://www.defensenews.com/industry/2018/11/27/vendors-showcase-defense-tech-for-frances-new-innovation-agency/.

162 Neurala, 'About Us', https://www.neurala.com/about.

163 Eze Vidra, '30 Machine Intelligence Startups to Watch in Israel', Medium, 15 February 2017, https://medium.com/@ediggs/30-machine-intelligence-startups-to-watch-in-israel-a05b6597c4a5.

164 Marcus Roth, 'AI in Military Drones and UAVs – Current Applications', Emerj, 30 January 2019, https://emerj.com/ai-sector-overviews/ai-drones-and-uavs-in-the-military-current-applications/.

165 Future of Life, 'An Ospen Letter to the United Nations Convention on Conventional Weapons', https://futureoflife.org/autonomous-weapons-open-letter-2017/.

166 See also https://en.wikipedia.org/wiki/Recognition.

167 Kari Paul, 'San Francisco is first US city to ban police use of facial recognition tech', 14 May 2019, https://www.theguardian.com/us-news/2019/may/14/san-francisco-facial-recognition-police-ban.

168 Erin Durkin, 'New York school district's facial recognition system sparks privacy fears', The Guardian, 31 May 2019, https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears.

169 Shazeda Ahmed, 'The Messy Truth About Social Credit', Logic Magazine no. 7, 2019, https://logicmag.io/07-the-messy-truth-about-social-credit/

170 See e.g. Chris Buckley and Paul Mozur, 'How China Uses High-Tech Surveillance to Subdue Minorities', The New York Times, 22 May 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html and 'How Mass Surveillance Works in Xinjiang, China', Human Rights Watch, 2 May 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang.

171 China's Algorithms of Repression - Reverse Engineering a Xinjiang Police Mass Surveillance App', Human Rights Watch, 1 May 2019, https://www.hrw.org/

report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

172 Linda Kinstler, 'Big tech firms are racing to track climate refugees', MIT Technology Review, 17 May 2019, https://www.technologyreview.com/s/613531/big-tech-firms-are-racing-to-track-climate-refugees/

173 Blake Schmidt and Venus Fang, 'The Companies Behind China's High-Tech Surveillance State', Bloomberg, 21 February 2019, https://www.bloomberg.com/news/articles/2019-02-21/the-companies-behind-china-s-high-tech-surveillance-state,

174 Paul Mozur, Jonah Kessel and Melissa Chan, 'Made in China, Exported to the World: The Surveillance State', The New York Times, 24 April 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

175 Blake Schmidt and Venus Fang, 'The Companies Behind China's High-Tech Surveillance State', Bloomberg, 21 February 2019, https://www.bloomberg.com/news/articles/2019-02-21/the-companies-behind-china-s-high-tech-surveillance-state,

176 Yuan Yang, 'China pours millions into facial recognition start-up Face++', Financial Times, 1 November 2017, https://www.ft.com/content/4d008d46-bed2-11e7-b8a3-38a6e068f464,

177 David Ramli and Mark Bergen, 'This Company Is Helping Build China's Panopticon. It Won't Stop There', Bloomberg, 19 November 2018, https://www.bloomberg.com/news/articles/2018-11-19/this-company-is-helping-build-china-s-panopticon-it-won-t-stop-there,

178 Ibid.

179 SenseTime, https://www.sensetime.com/about.html#company (Google translation).

180 Christian Shepherd, 'China's SenseTime sells out of Xinjiang security joint venture', Financial Times, 15 April 2019, https://www.ft.com/content/38aa038a-5f4f-11e9-b285-3acd5d43599e,

181 http://www.yitutech.com/en/intro/

182 Amanda Lentino, 'This Chinese facial recognition start-up can identify a person in seconds', CNBC, 16 May 2019, https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html,

183 CK Tan, 'Malaysian police adopt Chinese AI surveillance technology', Nikkei, 18 April 2018, https://asia.nikkei.com/Business/Companies/Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police,

184 Sarah Dai, 'Meet five Chinese start-ups pushing facial recognition technology into the mainstream', South China Morning Post, 20 February 2018, https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology,

185 Queenie Wong, 'Why facial recognition's racial bias problem is so hard to crack', CNet, 27 March 2019, https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/,

186 Paige Leskin, 'Amazon's public policy exec got booed in a meeting with New York council members when he evaded a question about the company's business with immigration agencies', Business Insider, 12 December 2018, https://www.businessinsider.nl/amazon-ice-government-provides-facial-recognition-tech-2018-12/; see also: ICRAC, 'Open Letter to Amazon against Police and Government use of Rekognition', https://www.icrac.net/open-letter-to-amazon-against-police-and-government-use-of-rekognition/,

187 Saqib Shah, 'Amazon joins Microsoft in calling for regulation of facial recognition tech', Engadget, 8 February 2019, https://www.engadget.com/2019/02/08/amazon-microsoft-facial-recognition-laws/,

188 https://www.research.ibm.com/artificial-intelligence/trusted-ai/diversity-in-faces/

189 See also Shannon Liao, 'IBM didn't inform people when it used their Flickr photos for facial recognition training', The Verge, 12 March 2019, https://www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training,

190 Katyanna Quach, 'While Google agonizes over military AI, IBM is happy to pick up the slack, even for the Chinese military', The Register, 12 April 2019, https://www.theregister.co.uk/2019/04/12/ibm_ai_database/,

191 Gerrard Cowan, 'Fast forward: Video analysis technology trend developments', Jane's International Defence Review, May 2019.

192 Natasha Singer, 'Microsoft Urges Congress to Regulate Use of Facial Recognition', The New York Times, 13 July 2018, https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html and https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

193 Synesis, https://synesis.by/en,

194 Nanalyze, 'The Top-10 Russian Artificial Intelligence Startups', 10 June 2018, https://www.nanalyze.com/2018/06/10-russian-artificial-intelligence-startups/,

195 TASS, 'The video monitoring system of the Skolkovo resident company entered the top technologies of 2017', 22 March 2018, https://tass.ru/ekonomika/5056415

196 Yarmak Taisiya, 'Skolkovo's startup VisionLabs raised $5.5 million in series A round from Sistema VC to expand its global solutions', 7 July 2016, https://sk.ru/news/b/pressreleases/archive/2016/07/07/skolkovo_2700_s-startup-visionlabs-raised-_2400_55-million-in-series-a-round-from-sistema-vc-to-expand-its-global-operations.aspx and http://www.ai-startups.org/country/Russia/,

197 Adrien Henni, 'After partnering with Facebook and Google, Russian startup VisionLabs raises $5,5 million from local corporate fund', Venturebeat, 7 July 2016, https://venturebeat.com/2016/07/07/russian-facial-recognition-startup-visionlabs-raises-5-5m-after-partnering-with-facebook-and-google/,

198 VisionLabs email, received 12 April 2019.

199 See e.g. Hugh Griffith, 'Bargain hunters: military forces eye innovative COTS UAV solutions', Jane's International Defence Review, April 2018.

200 Including use of commercially available types by non-state actors; see e.g.: PAX/ARES, 'Emerging Unmanned Threats: The use of commercially-available UAVs by armed non-state actors', February 2016, https://www.paxforpeace.nl/media/files/pax-ares-special-report-no-2-emerging-unmanned-threats.pdf. Also see: Scott Alexander, 'Follow the leader – US Army unmanned ground vehicle programmes', Jane's Defence Weekly, 17 April 2019.

201 Peter Burt, 'Off the leash – the development of autonomous military drones in the UK', Drone Wars UK, November 2018, https://dronewars.net/wp-content/uploads/2018/11/dw-leash-web.pdf.

202 Animal Dynamics, https://www.animal-dynamics.com/ and 'Biomimicry or bio-inspired design?', 19 April 2019, https://www.animal-dynamics.com/ad-blog/2019/4/10/biomimicry-versus-bio-inspired-design.

203 Animal Dynamics, 'Stork', https://www.animal-dynamics.com/stork-public

204 Animal Robotics email, received 23 April 2019.

205 Melanie Rovery, 'Autonomous Warrior', Jane's Defence Weekly, 13 March 2019.

206 Animal Dynamics, 'Skeeter', https://www.animal-dynamics.com/skeeter-project

207 Accelerated Dynamics, https://www.acceleratedynamics.co/,

208 Beth Stevenson, 'Animal Dynamics acquires autonomous software developer Accelerated Dynamics', Jane's Defence Weekly, 11 March 2019, https://www.janes.com/article/87127/animal-dynamics-acquires-autonomous-software-developer-accelerated-dynamics,

209 https://www.acceleratedynamics.co/products/swarm-manager/,

210 Animal Robotics email, received 23 April 2019.

211 Ibid.

212 Ibid.

213 Airobotics email, received 16 April 2019.

214 Airobotics, https://www.airoboticsdrones.com/

215 Steven Scheer, 'Israeli drone maker Airobotics raises $32.5 million in private funds', Reuters, 7 September 2017, https://www.reuters.com/article/us-israel-tech-airobotics/israeli-drone-maker-airobotics-raises-32-5-million-in-private-funds-idUSKCN1BI1T9,

216 'Airobotics Raises $32.5 Million in Round C to Meet Growing Demand in Mining and Homeland Security Industries', Airobotics press release, 7 September 2017, https://www.airoboticsdrones.com/press-releases/airobotics-raises-32-5-million-round-c-to-meet-growing-demand-in-mining-and-homeland-security-industries/ and Steven Scheer, 'Israeli drone maker Airobotics raises $32.5 million in private funds', Reuters, 7 September 2017, https://www.reuters.com/article/us-israel-tech-airobotics/israeli-drone-maker-airobotics-raises-32-5-million-in-private-funds-idUSKCN1BI1T9,

217 Keren Tsurial Harari and Meir Orbach, 'CEO of Automated Drones Company Airobotics Draws the Line at Airborne Firearms', CTech, 5 December 2018, https://www.calcalistech.com/ctech/articles/0,7340,L-3751434,00.html,

218 Ibid.

219 Heron Systems, 'About', http://heronsystems.com/about/

220 Heron Systems, 'MACE', http://heronsystems.com/products/multi-agent-cooperative-engagement-mace/,

221 Percepto, https://percepto.co/,

222 Ibid.

223 Ibid.

224 Percepto, 'Applications', https://percepto.co/applications/

225 Percepto email, received 15 April 2019.

226 ShieldAI, https://www.shield.ai/,

227 Ibid.

228 ShieldAI, 'Nova', https://www.shield.ai/nova,

229 WelcomeAI, 'Shield AI protects service members and innocent civilians with artificially intelligent systems', https://www.welcome.ai/tech/security/shield-ai,

230 Caitlin Irvine, 'Swarming Technology is Changing Drone Warfare – Part One of Three', The Security Distillery, 10 July 2018, http://securitydistillery.com/2018/07/10/swarming-technology-is-changing-drone-warfare-part-one-of-three/,

231 Thomas McMullan, 'How swarming drones will change warfare', BBC, 16 March 2019, https://www.bbc.com/news/technology-47555588,

232 Jessica Cussins, 'AI Researchers Create Video to Call for Autonomous Weapons Ban at UN', Future of Life Institute, 14 November 2017, https://futureoflife.org/2017/11/14/ai-researchers-create-video-call-autonomous-weapons-ban-un/

233 Roborder, 'Consortium', https://roborder.eu/partners/consortium/

234 Zach Campbell, 'Swarms of Drones, Piloted by Artificial Intelligence, May Soon Patrol Europe's Borders', The Intercept, 11 May 2019, https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/.

235 Zach Campbell, 'Swarms of Drones, Piloted by Artificial Intelligence, May Soon Patrol Europe's Borders', The Intercept, 11 May 2019, https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/.

236 Ibid.

237 Blue Bear Systems, 'Services', http://bbsr.co.uk/services.

238 Ibid.

239 '£2.5m injection for drone swarms', UK Government press release, 28 March 2019, https://www.gov.uk/government/news/25m-injection-for-drone-swarms.

240 Corenova Technologies, https://www.corenova.com/.

241 Corenova Technologies, 'Working Together', https://www.corenova.com/#partner.

242 DARPA, 'DARPA Seeks Proposals for Third OFFSET Swarm Sprint, Awards Contracts for Second', 12 October 2018, https://www.darpa.mil/news-events/2018-10-12.

243 Tamir Eshel, 'DARPA Studies Human-Swarm Interactions', Defense Update, 14 October 2018, https://defense-update.com/20181014_swarm_sprint.html

244 DARPA, 'OFFensive Swarm-Enabled Tactics (OFFSET)', https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics.

245 Amit Malewar, 'DroneBullet, a kamikaze drone missile can eliminate the aerial threats', Tech Explorist, 6 May 2019, https://www.techexplorist.com/dronebullet-a-kamikaze-drone-missile-can-eliminate-the-aerial-threats/22877/

246 Robin Hughes, 'AerialX unveils intuitive CUAS development', Jane's Missiles & Rockets, 23 May 2019, https://www.janes.com/article/88754/aerialx-unveils-intuitive-cuas-development.

247 Robin Hughes, 'Machine Vision', Jane's Exhibition News, 29 May 2019, https://www.janes.com/article/88839/machine-vision-cs19d1.

248 Ibid.

249 Robin Hughes, 'AerialX unveils DroneBullet CUAS development', Jane's International Defence Review, July 2019.

250 'U.S. Air Force Teams with Citadel Defense to Defeat Weaponized Drones', Citadel Defense press release/PRNewswire, 2 May 2019, https://www.prnewswire.com/news-releases/us-air-force-teams-with-citadel-defense-to-defeat-weaponized-drones-300839155.html.

251 Citadel Defense, https://www.dronecitadel.com/.

252 UAS Vision, 'Citadel Defense Wins $1M Counter Drone Contract', 18 April 2019, https://www.uasvision.com/2019/04/18/citadel-defense-wins-1m-counter-drone-contract/.

253 'U.S. Air Force Teams with Citadel Defense to Defeat Weaponized Drones', Citadel Defense press release/PRNewswire, 2 May 2019, https://www.prnewswire.com/news-releases/us-air-force-teams-with-citadel-defense-to-defeat-weaponized-drones-300839155.html.

254 Citadel Defense, 'A Counter Drone System You Can Trust', https://www.dronecitadel.com/features.php.

255 Ibid.

256 Airspace, https://airspace.co/.

257 Airspace, 'Airspace Systems Raises $20M to Guard Critical Infrastructure, Public Space and the Military from Enemy Drones', 12 March 2018, https://airspace.co/news/Critical_Infrastructure.html.

258 Ibid.

259 'iRobot Awarded $3 Million for PackBot EOD Robots and Services', iRobot news release, 31 July 2006, http://investor.irobot.com/news-releases/news-release-details/irobot-awarded-3-million-packbot-eod-robots-and-services.

260 Military work was then continued by Endeavor Robotics, which was subsequently taken over by FLIR in 2019. FLIR and its autonomous military robots will be covered in a later report focusing on the arms industry.

261 https://www.visionfund.com/portfolio and Andrew Torchia, Stephen Kalin, Marwa Rashad, 'Saudi's PIF invested in 50-60 firms via SoftBank fund: director', Reuters, 23 October 2018, https://www.reuters.com/article/us-saudi-investment-pif/saudis-pif-invested-in-50-60-firms-via-softbank-fund-director-idUSKCN1MX12X.

262 Tim Bradshaw and Kana Inagaki, 'SoftBank to buy Boston Dynamics from Alphabet', Financial Times, 9 June 2017, https://www.ft.com/content/22827134-4cb2-11e7-a3f4-c742b9791d43.

263 Nick Statt, 'Alphabet agrees to sell Boston Dynamics to SoftBank', The Verge, 8 June 2017, https://www.theverge.com/2017/6/8/15766434/alphabet-google-boston-dynamics-softbank-sale-acquisition-robotics.

264 SoftBank email, received 24 May 2019.

265 Barbara Opall-Rome, 'Pentagon Fast-Tracks Fielding of Israeli-Designed Robot', Defense News, 20 October 2013.

266 Roboteam, 'About Us', http://www.robo-team.com/about-us/.

267 Barbara Opall-Rome, 'Israel Debuts Micro Robot in Anti-Tunnel Campaign', Defense News, 28 July 2014.

268 Barbara Opall-Rome, 'Israeli Start-Up Snags USAF EOD Robot Award', Defense News, 20 September 2015, http://www.defensenews.com/story/defense/policy-budget/industry/2015/09/20/israeli-start-up-snags-usaf-eod-robot-award/72519514/.

269 Courtney E. Howard, 'Roboteam Artificial Intelligence Control Unit brings autonomous, facial recognition, AI to UAS operation', Intelligent Aerospace, 2 March 2018, https://www.intelligent-aerospace.com/military/article/16544909/roboteam-artificial-intelligence-control-unit-brings-autonomous-facial-recognition-ai-to-uas-operation.

270 Matt O'Brien, 'Israeli firm caught up in the US-China rivalry over military robots', Times of Israel, 28 December 2018, https://www.timesofisrael.com/israeli-firm-caught-up-in-us-china-rivalry-over-military-robots/ and Tofi Stoler, 'Israeli and U.S. Defense Robotics Companies Quarrel Over China Ties', CTech, 1 August 2018, https://www.calcalistech.com/ctech/articles/0,7340,L-3743543,00.html.

271 Roboteam, 'About Us', http://www.robo-team.com/about-us/.

272 General Robotics, 'About Us', http://www.glrobotics.com/about-us.

273 General Robotics, 'Pitbull', http://www.glrobotics.com/pitbulllightweaponstation.

274 Barbara Opall-Rome, 'Introducing: Israel 12-Kilo Killer Robot', Defense News, 8 May 2016, https://www.defensenews.com/global/mideast-africa/2016/05/08/introducing-israeli-12-kilo-killer-robot/.

275 Seth J. Frantzman, 'Watch this Israeli robot face off against a marksman in a live-fire demo', Defense News, 31 May 2019, https://www.defensenews.com/unmanned/2019/05/31/watch-this-israeli-robot-face-off-against-a-marksman-in-a-live-fire-demo/

276 General Robotics email, received 15 April 2019.

277 Union of Concerned Scientists, 'Self-Driving Cars Explained', last revised 21 February 2018, https://www.ucsusa.org/clean-vehicles/how-self-driving-cars-work.

278 Ibid

279 Kelsey D. Atherton, 'Are Killer Robots the Future of War? Parsing the Facts on Autonomous Weapons', The New York Times, 15 November 2018, https://www.nytimes.com/2018/11/15/magazine/autonomous-robots-weapons.html.

280 https://en.wikipedia.org/wiki/DARPA_Grand_Challenge

281 See e.g. Scott Alexander, 'Follow the leader – US Army unmanned ground vehicle programmes', Jane's Defence Weekly, 17 April 2019.

282 Yasmin Yablonko and Dubi Ben-Gedalyahu, 'Israeli car laser sensors co Innoviz raises $132m', Globes, 26 March 2019, https://en.globes.co.il/en/article-startup-up-innoviz-raises-132m-1001279636.

283 Automoblog, 'Israeli Company Utilises Military Background for Autonomous Cars', 29 September 2017, https://www.automoblog.net/2017/09/29/israeli-company-utilizes-military-background-for-autonomous-cars/.

284 Arbe Robotics, http://www.arberobotics.com/.

285 Reuters, 'IDF's Expertise Drives Tech Boom for Driverless Cars', 27 May 2018, https://www.haaretz.com/israel-news/idf-s-expertise-drives-tech-boom-for-driverless-cars-1.6117396.

286 Arbe Robotics email, received 10 July 2019.

287 Dibotics, http://www.dibotics.com/.

288 Pierrick Arlot, 'Défense et sécurité : six start-up rejoignent le programme de soutien Generate du Gicat', L'Embarqué, 6 March 2018, https://www.lembarque.com/defense-et-securite-six-start-up-rejoignent-le-programme-de-soutien-generate-du-gicat_007281 and https://www.gicat.com/__trashed/?lang=en.

289 Future of Life, 'An open letter to the United Nations Convention on Conventional Weapons, https://futureoflife.org/autonomous-weapons-open-letter-2017/.

290 Ariel Conn, 'AI Companies, Researchers, Engineers, Scientists, Entrepreneurs, and Others Sign Pledge Promising Not to Develop Lethal Autonomous Weapons', Future of Life Institute, 18 July 2018, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/.

291 See e.g. Ariel Conn, 'AI Companies, Researchers, Engineers, Scientists, Entrepreneurs, and Others Sign Pledge Promising Not to Develop Lethal Autonomous Weapons', Future of Life Institute, 18 July 2018, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/.

Sint Jacobsstraat 12
3511 BS Utrecht
The Netherlands

www.paxforpeace.nl
info@paxforpeace.nl

+31 (0)30 233 33 46
P.O. Box 19318
3501 DH Utrecht
The Netherlands