Summary ‘Don’t be evil?’

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
- Hardware
- AI software and system integration
- Pattern recognition
- Autonomous (swarming) aerial systems
- 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, and including 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.

Table 1: Companies surveyed for this report

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	-	

Company	Best practice	Medium concern	High concern	HQ	Relevant technology	Relevant military/security projects	Commit to not develop
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.
- means '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.