From Robots to Warbots: Reality Meets Science Fiction

From Robots to Warbots: Reality Meets Science Fiction

The ongoing robotization of armed forces raises concerns about the desirability of autonomous systems with lethal capacity. In contrast, unarmed military robots have already improved and supplied capabilities unconstrained by human physical limitations. But despite the long-term efforts to develop fully autonomous systems, no military robot can lift the fog of war.

By Dominika Kunertova

The 1920 play "R.U.R." by Czech writer Karel Čapek introduced the term "robot", derived from the word *robota*, meaning labor or servitude. Echoing Mary Shelley's novel Frankenstein from one century earlier, Čapek's dystopian story about mass production, dictatorships, and post-human beings depicted robots not as mechanical devices but as artificial biological anthropoid organisms that can eventually develop self-awareness and experience human emotions. In contrast, today, robots are widely understood as unmanned machines with a certain degree of automation and, increasingly, autonomy (see Box).

Activists opposing lethal autonomous weapons stage a protest at Brandenburg Gate in Berlin, Germany, March, 21, 2019. *Annegret Hilse / Reuters*

Once science fiction, robots have become part of everyday life: from automated vacuum cleaners to industrial product manufacturing. From dumb landmines to sophisticated military drones, in space and oceans, military robots have been widely deployed for dull, dirty, and dangerous missions, mostly to avoid putting their human creators into harm's way. Yet, they may have a reputation problem as ever greater levels of autonomy coincide with lesser human control over machines that have acquired the ability to not only destroy things but also kill people. How worried should we be about the military using robotic systems? Although observing the increasing use of military robots and their eventual employment in combat situations, the reality of killer robots is far from materializing anytime soon.

While most robots had only automated capabilities, advancements in commercial dual-use technologies, such as computing and communication, have significantly boosted the software that makes the robotic systems "alive." The cross-cutting Artificial Intelligence (AI) – and its main components, machine learning (algorithms) and big data (digital content) – is the key that can qualitatively enhance the autonomy of robots. Yet the apocalyptic visions of autonomous machines engaging in the full spectrum of military operation tend to overestimate what military applications of AI can achieve. For the time being, machine intelligence can decide and operate autonomously only in a narrowly defined area.

Technological innovation must go hand in hand with changes in the use of force. The robotization of armed forces widens the range and frequency of interactions between humans and robots. This creates a problem of trust in robots' reliability and efficiency due to persisting algorithm and data vulnerabilities.

Over the next decade, AI-enabled autonomy, faster computing, and better sensors will continue to improve the functional performance of existing robotic systems and will introduce new combat roles. The shift to the age of robots may be expected in the mid- to long term with new operational concepts of hybrid human-machine teaming and effectively networked swarms of lower-cost systems. Yet, robotic systems will not provide advantages beyond the tactical level – the warbots of tomorrow will remain strategically worthless.

Military Robots of Today

The study of military robotics is plagued by a conundrum of definitions as to what is understood by a "robot." Unmanned does not automatically mean autonomous because a machine can be remotely piloted and thus remains under the direct control of a human operator. This led some experts to conclude that unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and unmanned surface/underwater vehicles (USVs, UUVs) are not robots. Others claim that AI-powered systems are a whole new category distinct from a robotic system. *Ad abstractum,* robots do not even have to be mobile steel machines; for instance, robots in cyberspace like the voice assistant *Siri.*

Robotic systems will not provide advantages beyond the tactical level.

While using the terms "automatic/automated" often interchangeably, military robotics experts differ on how to define "autonomy." Often, they tend to grasp these terms by referring to the degree of "meaningful human control." Importantly, autonomy is not a binary term but a classifier, as it can have different effects in terms of tasks, functions, and the machine's relation to humans (see Box). If unmanned remotely operated vehicles are not robots, then only fully autonomous systems can be called robots. This distinction has no practical use since fully autonomous machines do not exist – robots cannot act with complete independence from human commands.

Automatic, Automated, Autonomous

When is a machine automatic, automated, or autonomous?

Automatic systems respond in a mechanical way to external inputs. Usually triggered by a tripwire, automatic functions are of the stimulus-response type, such as landmines, and are without any ability to discriminate the inputs.

Automated systems execute commands in a chronological pre-programmed way with sensors that help sequence the action. Although these systems have a greater degree of contingency, they are limited by algorithms that determine their rules of operations and behavior out of fixed alternative actions, which makes them predictable. Automated functions typically include calculations and computations.

Autonomous systems can choose between multiple options for action based on sensory input and can achieve goals through optimizing along a set of parameters. Although still constrained by pre-programmed range of actions, they can exercise independent judgment about courses of action to comply with the higher-level intent. Most experts agree that autonomy is not dichotomic and that referring to different degrees of autonomy is more accurate. Scharre and Horowitz's three-dimensional autonomy introduces important nuances: (a) the human–machine command-and-control relationship; (b) the sophistication of the machine; and (c) the types of decisions or functions being made autonomous (see selected sources). This means that a) hierarchically, machines can be semi-autonomous (human in the loop), human-supervised autonomous (human on the loop), or fully autonomous (human out of the loop); b) technically, one can distinguish automatic and automated functions from autonomous and "intelligent"; and c) functionally, the division of decision-making between the machine and the human accords with the nature of the task based on the levels of risks and engagement. This holistic understanding helps determine where the human is located relative to the loop and thus the degree of the machine's autonomy.

Military applications of robotic systems may already seem quite science-fiction-esque, yet their functional autonomy is still limited to non-critical functions such as mobility, interoperability, intelligence, surveillance, and reconnaissance (ISR), logistics and maintenance. Militaries opt for a machine with autonomous functions when an operator's cognitive capabilities are not essential. In terms of mobility with little or no supervision, machines perform autonomous take-off and landing and navigate with pre-programmed maneuvers, mainly when communication is difficult due to weather conditions, topography, or is simply denied. In terms of the targeting process, humans remain either in the loop of automated target recognition systems, for instance, when the target is too fast or beyond the operator's visual range, and when the system can detect, track, prioritize, and select targets autonomously but a human ultimately decides to engage the target. Some systems can operate under supervision with a human on the loop and engage with targets without the direct involvement of a human operator. However, this is limited to situations where the response window would be too short for humans to act, such as for the protection of ships or troops against incoming projectiles. Robotic systems capable of engaging targets with humans out of the loop are not yet operational (see selected sources).

Most military UAVs are small drones that provide tactical ground surveillance and transmit real-time information for troops to "see beyond the hill." The primary function of current-generation drones are still ISR missions, which they conduct with humans mostly supervising on the loop. Drones also proved useful as refueling tankers. Armed drones deployed in strike operations during the last twenty years are not flying killer robots, as nothing is more manned than an unmanned system: a fleet of four MQ-9 Reapers requires a two hundred crew of pilots, sensor operators, intelligence analysts, and lawyers.

UGVs unburden humans from tedious and risky tasks. Assigned with roles in logistics, training, area protection, intelligence, and reconnaissance, they provide important tactical support to ground forces. UGVs became popular for clearing roads and fields from mines. Explosive ordnance disposal has for example been a key mission for small ground robots in Iraq and Afghanistan. UGVs can also detect weapons at checkpoints, inspect buildings, secure areas within known perimeters such as military camps and borders, or simply carry equipment.

Underwater robots have proven useful for oceanic exploration, mine countermeasures (mine hunting and demining), and clandestine environmental reconnaissance. Navies are now experimenting with USVs and

UUVs of different sizes: while smaller ones can be deployed from manned ships and submarines to extend their operational reach, larger ones are deployed directly from pier to perform "manned" missions.

Warbots of Tomorrow

Military robots are becoming more autonomous thanks to the advances in big data analytics and machine learning algorithms. AI thus acts as a crucial capability enabler in command and control, ISR, training, and logistics (see CSS Analyses no.251). Together with faster computing and better sensors based on quantum technologies, this will lead to improving existing functions and integrating new concepts in robotic systems.

Future drones will fly longer, faster, farther, and monitor larger areas. They will get improved collision avoidance and automated safety features. UGVs will become robotic mules, and large multi-mission USVs will be fully integrated into naval operations. Future robots will timely collect, process, and preserve the integrity of data across operational domains to generate multi-source intelligence. They will not only collect, but also analyse data with onboard data-processing software. While robots recognize and evaluate only large objects, autonomous functions in defense will improve the system's sensitivity to distinguish smaller objects like drones from a bird and help to act fast in order to stop an attack by saturation. Some UAVs will get low-cost: cheaper, simpler, and expendable flying robots, such as the XQ-58 Valkyrie, will enable armed ISR in contested airspace.

Greater autonomy will also expand the functional range of robotic systems to combat missions. Future combat drones will be able to penetrate adversary's air defenses and operate in contested airspace. As no fully autonomous combat drone is close to becoming operational, these drones will assume the role of a loyal wingman within an air combat cloud. Unarmed ISR drones have already been used to enable lethal strikes by other weapon systems. While the War on Terror in the early 2000s facilitated the dronification of air strikes by the United States and the United Kingdom, French, Russian, Turkish, and Iranian armed drones have been recently combat-proven in Africa, Syria, Nagorno Karabakh, and Yemen. The interest in UGVs is shifting from logistics into combat as well. Although the first experiments date back to the 1930s Soviet wireless remotely controlled unmanned tanks (teletank project), only recently modern weaponized UGVs like the MUTT (Multi-Utility Tactical Transport) and THeMIS (Tracked Hybrid Modular Infantry System), demonstrated their ability to project combat power with anti-tank missiles and provide direct fire support.

Furthermore, human and machines will team up into the emerging hybrid capability of semi-autonomous robotic wingmen that will accompany crewed platforms to expand their capabilities by, for instance, carrying additional payloads as a flying missile magazine or a "third eye" with additional sensors. European future air combat systems projects do include the robotic wingman component (see CSS Analyses no.291). Although AI-based swarm capability is still out of reach, less intelligent deployment of vehicles *en masse* with multi-vehicle control represents innovative weapon delivery. Such a cooperative group of robotic systems that autonomously self-organizes to achieve a task will enable new operating methods. One can imagine a pilot commanding swarms of drones that fly ahead of the manned aircraft and perform area reconnaissance, like the Pentagon's Perdix experiment with micro-drones for aerial surveillance dropped out of F/A-18 Super Hornets. Swarming on the ground will also take form of convoying and detecting explosive devices.

> Military applications of robotic systems are still limited to non-critical functions.

And Then Killer Robots, Right?

The ongoing robotization of armed forces raises questions about the desirability of autonomous systems with lethal capacity. Lethal autonomous weapon systems (LAWs) are understood as fully autonomous weapons that can decide about selecting and engaging targets based on sensor inputs and without human control. Academics, legal scholars, and policymakers are vigorously debating whether the advent of LAWs will bring about a "robopocalypse" of dehumanized warfare and how this should be prevented.

The military remains skeptical about weaponizing fully autonomous robots: no military commander would want to deploy robotic machines if they were known to breach the chain of command (reliability) and execute tasks based on corrupt data (efficiency). Applying AI in military robotic systems faces important limitations that plague intelligent robotic machines today largely due, paradoxically, to the lack of intelligence.

AI-driven robots are only as good as the parameters they work with and the data they are fed on. Modern AI is largely based on machine learning, which, thanks to ever more powerful computers and greater data availability, prompts systems to build complex statistical models of the world based on probabilistic reasoning. While these algorithms excel in finding patterns in data, such as image-recognition, classification, or translation, they cannot grasp a wider understanding of reality and make judgments. This narrow AI enables robots to perform tasks for which they were trained. Only machines with a general AI would be able to think for themselves and develop their own courses of action. However, general AI does not yet exist. Robots trained to perform a specific task can outperform humans, yet a new threat environment will render these systems useless. Also, since they are human-made, flaws and biases are always a possibility.

The challenge extends from algorithm to data bias. It matters how data are generated, collected, processed, analyzed, who has access to these data and meta-data, and who interprets them. Rogue datasets affect the output and create machine learning algorithmic bias (see selected sources). Soldiers may over-rely on machines and gain a false sense of security without fully comprehending how such systems reach their judgments. This is known as "automation bias." Furthermore, trusting robots too much may decrease the confidence in human problem-solving ability. This opens the debate whether any meaningful human control (in non-technical sense) is possible.

These concerns make the decision to weaponize AI outright dangerous not only for ethical and legal but also for operational reasons. Full autonomy will make robots unpredictable and even unwanted since they would likely break the chain of command and escape any liability and accountability. The epistemic community of the *UN Convention on Certain Conventional Weapons* has been discussing the governance rules for LAWs. The main obstacle to curbing unintended consequences of fully autonomous military robots, and to banning LAWs, is the fact that they do not exist yet.

Expect Robopocalypse on Another Day

Greater levels of autonomy will improve functionality and safety measures in robotic

Selected Sources

Michael C. Horowitz / Paul Scharre, "Meaningful Human Control in Weapon Systems: A Primer," *Center for a New American Security,* 2015.

Vincent Boulanin / Maaike Verbruggen, "Mapping the Development of Autonomy in Weapon Systems," *SIPRI,* 2017.

Arthur Holland Michel, "Known Unknowns: Data Issues and Military Autonomous Systems," *United Nations Institute for Disarmament Research,* 2021.

Kenneth Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict,* London: Hurst, 2021.

systems in the short-term, while robotic wingmen will provide operational support to crewed platforms in the mid- to long-term. However, fully autonomous weapons with lethal capacity are unlikely to be operational in the short- to mid-term, also because they might simply get banned. The expectations about the military utility of autonomous robots need to be nuanced. These systems cannot strategize, nor can their computing power or superior fighting capacities make warfare more predictable. Autonomous weapons get dumbed by the fog of war.

With the advances in AI and ever more powerful machine learning, robotic machines with varying levels of sophistication, range of tasks, and human control/oversight will continue to permeate armed forces, significantly increasing human-robot interactions. This brings attention to another literary piece introducing a different set of "laws." While Čapek described the unique robot-human relationship, in 1942 Isaac Asimov prescribed an acceptable behavior of robots. His three laws of robotics stipulate that robots may not injure humans, including through inaction, that robots must obey orders by humans except if such orders lead to harming humans, and that robots must protect their own existence, yet only if respecting the first two laws.

In military robotics, this becomes problematic once robots are deployed on the battlefield. Formulating a 21st-century version of robotic laws runs into the problem of thresholds and definitions, such as how a robot can differentiate between harming a combatant from a civilian or how to program human concepts like unnecessary suffering (see selected sources). Most importantly, for robots to follow any laws, AI still needs substantial advancements.

Undeniably, AI is a new buzzword that will bring important evolutionary changes to how armed forces do warfare. Yet, just like hypersonic weapons and the information technology boom before, AI is not going to revolutionize military affairs. Understanding the persisting limitations of robots should help the military avoid tasking these systems with inappropriate missions and deploying them prematurely. As the old Georges Clemenceau's saying goes, war is too important to be left to the killer robots.

For more on perspectives on Military Doctrine, see CSS core theme page.

Dominika Kunertova is a Senior Researcher in the Global Security Team at the Center for Security Studies (CSS) at ETH Zürich

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Fabien Merz
Language editing: Henrik Larsen
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000508358