Federal Academy
for Security Policy

Security Policy Working Paper, No. 23/2017

Autonomous or semi-autonomous weapons systems
A potential new threat of terrorism?

by Wolfgang Rudischhauser

Autonomous weapons systems currently developed by the military and by private companies, and their proposed ban, have received high attention in media and security circles. A much more concrete threat are existing semi-autonomous or guided systems, such as "Drones" or Unmanned Ground Vehicles which are already used or tested by terrorist groups, such as ISIL, in various war theatres. Access to these technologies is getting easier every day and their commercial use will increase exponentially in the near future. Much more attention should therefore be paid to the risk of them being used for terrorist attacks, in particular if they are used to spread chemical, biological or radiological material in order to receive additional attention. We need to be prepared that in the near future terrorists will not only use knives, improvised explosives or trucks to spread fear, but will increasingly rely on more sophisticated technologies.

In a most recent paper published and signed by nearly one hundred specialists in Artificial Intelligence (AI) and leaders of high-tech companies, among them Tesla founder Elon Musk and Google researcher Mustafa Suleyman, the authors have warned against the risks of autonomous weapons systems (so called "killer robots"). They called for them to be banned under the United Nations Weapons Convention as they would dramatically change wars of the future. There is an ongoing intense ethical debate on whether these weapons can be legal under international humanitarian law. Some experts also warn of the risk that these weapons systems could make asymmetric wars easier between states and for non-state actors (such as terrorists). Will they become a new form of terrorist threat?

These days, terrorist attacks, such as in Barcelona, Brussels, London, Nice or Berlin are committed with free access weapons, such as knives, improvised explosives or even trucks running into large crowds. While these attacks need to be strongly condemned as they killed or injured many innocent people, our look should also go beyond, towards more sophisticated weapons that can potentially have an even larger impact, let alone psychologically. We should look more closely at new types of weapons such as drones or other unmanned vehicles, whether guided or autonomous, that can potentially be used for both hybrid warfare tactics and terrorist attacks.

Drones or "Unmanned aerial vehicles (UAVs)" as they are often referred to, are already in use not only by states, but also increasingly by non-state actors, such as ISIL, in various theatres.[1] They are used for surveillance purposes, but also to kill. ISIL allegedly has even been using UAVs to disperse Chemical weapons and toxic chemicals, although supporting evidence remains vague. The Pentagon has recently launched a 700

[1] Yayla, Ahmet (2017): The Potential Threats Posed By ISIS's Use Of Weaponized Air Drones And How To Fight Back, in: Huffington Post, https://www.huffingtonpost.com/entry/the-potential-threats-posed-by-isiss-use-of-weaponized_us_58b654b3e4b0e5fdf6197894

million dollar crash programme to identify measures to counter this threat – reportedly so far with mixed results.[2] Although hybrid warfare scenarios often build on the use of the same disruptive and chaos-creating acts, similarly to those used by terrorists, this paper will focus on the latter risk.

Do we need to look at an entirely new threat for our security? To what extent will non-state groups have access to new devices, including autonomous technologies? Would they be tempted to use them for their attacks, and if so, in what kind of terrorism-related scenario would the use of such technologies be an advantage for the attacker? What are the crucial technological advancements that would have to be closely monitored by those responsible for our populations' security?

Low tech or high tech: differing ramifications of unmanned systems

Full autonomy of new weapons systems is still more a vision than a reality. There is an intense debate among experts, whether fully autonomous systems are already being developed successfully – no matter whether at the military level or in the private industry. Some experts suggest that there should never be such things like fully autonomous systems as man always should be in control of them. Humanitarian Law and other fundamental law principles are invoked. Banning these weapons or restricting their development might be a solution for very sophisticated systems and full autonomy based on AI. It is important therefore to distinguish between full autonomy which includes autonomous decision making and "automation" or semi-autonomy, already in use with UAVs. The latter technology need to be looked at in particular as due to its large availability and commercial use, banning is not any longer an option.

Some of the technologies emerging around unmanned systems and autonomy of delivery systems are rather low-tech. They include small electro motors, low-end sensors like cameras, acoustic, heat and pressure sensors, electronics and processors, lightweight materials (such as carbon fiber), communication systems and programming guides for automated systems. All of them are within reach also of non-state actors or terrorist groups. Small drones, so called do-it yourself (DIY) or "hobby drones" can be bought in the supermarket around the corner, and even our kids can fly them.

Relevant technologies are constantly being improved and are becoming cheaper and increasingly available on the open internet or on the "dark net" every day. They are close to impossible to control because they often represent off-the-shelf civilian technology with nearly infinite purposes. A simple and rather crude, small weaponized drone can be built with these components and can be used remotely controlled or automated, with a predefined target. The casualty impact of such drones would be rather low unless they are combined with chemical, biological, radiological material or high impact explosives (CBRe), which comes with additional difficulties. However, they could cause a lot of panic if used at large public events such as rock concerts or in football stadiums. They would be very difficult to defend against, due to their small size, especially if used in larger numbers simultaneously. Jamming or spoofing are among the possible countermeasures currently explored, including by the Pentagon. Also more conventional measures, such as guns could be employed against them, but the latter carry the risk of serious collateral damage. Some countries therefore even consider using animals such as eagles or buzzards to take small drones down without harm. This would not, however be efficient against larger numbers of small drones or so called drone "swarms", which are very difficult to tackle successfully.

Other emerging technologies in the field are rather on the high-end side. These include truly capable unmanned systems to take decisions autonomously – especially autonomous targeting – as well as more sophisticated, stronger and faster propulsion systems, durable materials such as titanium and aircraft-grade aluminium, high-end sensors (night-vision, thermal imaging, radar, laser range finder), small dispersion means, fit for chemical and biological material, autopilot software for heavier or more complex aerial vehicles and larger payloads, high capacity and lightweight batteries, autonomy software and small high end

[2] The New York Times (2017): Pentagon tests tech to combat ISIS Drones (26 September), p.1.

processors. Fortunately, sophisticated swarm technologies, although under development both by military and by private companies, are currently not (yet) accessible to non-state actors. The added value of UAV swarms both in relation to costs and efforts can be considered out of proportion for terrorist purposes.

Problems and roadblocks for a potential use of these technologies in terrorist attacks

The payload of affordable consumer-market UAVs is still much too small to transport larger quantities of explosive or CBRe materials. In addition, materials that are dangerous enough to target larger crowds in small quantities (like certain chemical or biological toxins) would need to be dispersed broadly to be effective. Yet, with private companies such as Amazon experimenting with and introducing at bigger scale “delivery” drones with larger payloads, this can change rapidly. The acquisition or diversion of these drones for malicious purpose (like their “hijacking” by terrorist or other non-state actor groups) is becoming an ever more realistic threat.

As outlined, and although technology rapidly advances both in terms of artificial intelligence (autonomous decision making) and hardware, completely autonomous armed UAVs still have not been developed even within the most advanced militaries, and software to control the vehicles is not yet publicly accessible. Many other systems involving autonomy such as “Google cars” or “flying taxis” are still in an experimental phase and expensive. However technology evolves very fast and many of these systems will become cheaper and increasingly available for civil and private users. Currently they are still produced and sold by a limited number of manufacturers and retailers. This makes it potentially easier to control and track them and involves a particular responsibility on part of industry and researchers. Western countries still have a competitive edge, which allows setting standards for control.

Nevertheless it cannot be ruled out that a well-funded and well-organized terrorist group with large training capacities and intellectual manpower, such as ISIL, will get hold of them, now or in the near future. They could either build or otherwise acquire a sophisticated drone or other delivery means to be used for an automated or human-guided attack against more hardened targets such as power plants, water works and other critical infrastructure or military installations. It is therefore worthwhile to reflect on how their proliferation can best be controlled before they are introduced rather than thereafter.

How would these technologies change the risk-taking calculus of terrorists?

Fortunately, as demonstrated in recent terrorist events, sophistication is currently not high on the mind of terrorist groups. And it is even more unclear whether larger or more sophisticated drones or autonomous vehicles, whether airborne, seaborne or land borne, would provide them with much advantage over low-tech ones – besides higher speed, payload and accuracy. The manufacturing process of more sophisticated systems would for sure be much harder to conceal and more expensive. Their use therefore would depend on the terrorist group’s capabilities and finances, and whether the increased payload, autonomy and larger attainable targets would justify the effort. Provided that fully autonomous systems become more broadly available, the central question is, under what circumstances would an effort to acquire a truly autonomous system be worthwhile for a non-state actor or terrorist group? And, given that expensive and sophisticated technology is becoming increasingly available, at what point in the future might their economic calculus change?

Autonomy (or at least semi-autonomy) carries a number of advantages for terrorists as it reduces the perpetrators’ own casualties. Let’s for a moment imagine that an unmanned ground vehicle (UGV) would have been used in the attacks at Nice, Berlin or Barcelona instead of a truck. Not only would they have been much harder to stop, given that there would have been no driver on board. There would also have been no need for attackers risking their lives, and attribution to a perpetrator or a group would be much more difficult. Similarly, UAVs used for terrorist attacks to deliver explosives or disperse certain CBRe agents do not need to be fully autonomous, but can still protect the perpetrator from being directly involved. Automation of release and autonomous orientation to reach the target, technologies already in use for example in cruise missiles, are sufficient. The UAV does not need to take autonomous decisions for these kinds of manoeuvres. Hence, this scenario is probably more realistic, given that "standard" UAVs are cheap and can rely on well-developed and tested technology. It is even possible that a drone would simply be remotely controlled by terrorists. However, the risk of detection (or interference by GPS "spoofing") is much higher in this case. While finding volunteers ready to give up their own life during terrorist attacks does not seem to be a problem for some groups (one example are the radicalized supporters of ISIL), smaller or more centrally organized groups might have a different calculus. As unmanned or at least semi-autonomous cars and trucks are expected to be market-ready in the next five to ten years, those can be considered another potential new threat.

Future risks: questions to be addressed

As outlined, many of the technologies developed or needed for fully autonomous or semi-autonomous weapons systems are still not publicly available or difficult to access for terrorist groups. However, new systems that could be used for terrorist attacks, such as drones or UGVs are already available or will become a reality soon. Therefore it is prudent to look more closely at these particular technologies when considering future risks. Also questions of cost-benefit calculations for terrorists, as well as of the possibility of controlling the spread of technologies need to be addressed, such as:

- In which terrorism-related scenarios would the use of UAV/UGVs be an advantage for the attacker? What added value would autonomy of these delivery vehicles bring to them?
- Would autonomy make it more difficult to identify and link them to a specific terrorist group?
- What are the crucial technological advancements that need to be watched, in particular regarding UAVs? How can uploading of autonomy software on otherwise non-autonomous systems be restricted? How can autonomous UAVs/UGVs be secured against abuse on the manufacturing level?
- From where could terrorists acquire autonomous systems? What can be done to prevent non-state actors to develop autonomous vehicles themselves, once the technologies become "democratized"?
- What would be potential countermeasures to stop UGVs/UAVs? How can they be employed (in an urban environment)? Is there a reliable jamming/disabling/spoofing technology that can stop them and to whom should it be made available?
- How big is the difference in the threat level and proliferation risks of emerging low and high tech related to UAVs and autonomy? Do they need different measures to be controlled? Should efforts be put into controlling either low or rather high-end technologies? Which one carries the higher risk?
- Should efforts concentrate on controlling technologies revolving around unmanned systems and autonomy itself due to their potential for changing "warfare"? Or should it rather concentrate on preventing their misuse for malicious purposes, such as using them as vectors for spreading CBRe materials?

While many question marks remain to be addressed, the security risks that stem from autonomous or semi-autonomous technologies being used by terrorists fortunately remains low at this stage. Knives, guns, improvise explosive devices and cars/trucks will remain for the time being the primary means in terrorist attacks, at least for less organized groups or radicalized single perpetrators. It is nevertheless advisable to look at how new technologies being developed or becoming more accessible to non-state actors and terrorists might change our threat assessment in the future.

Wolfgang Rudischhauser[3] is the Vice President of the Federal Academy for Security Policy in Berlin.

[3] Jean Backhus and Stefan Maetz, former interns at NATO, have contributed with their reflections or comments to this article. The article nevertheless reflects the author's personal opinion, and neither their, nor the viewpoint of the Federal Academy for Security Policy.